PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 17/60, 1/00

A1

(11) International Publication Number: WO 00/62220

(43) International Publication Date: 19 October 2000 (19.10.00)

(21) International Application Number: PCT/US00/10066

(22) International Filing Date: 13 April 2000 (13.04.00)

(30) Priority Data:

60/129,283	13 April 1999 (13.04.99)	US
60/129,011	13 April 1999 (13.04.99)	US
09/335,443	17 June 1999 (17.06.99)	US
09/546,805	11 April 2000 (11.04.00)	US

(71) Applicant: ILUMIN CORPORATION [US/US]; Suite 3000, Building D, 1506 N. Technology Way, Orem, UT 84097 (US).

(72) Inventors: BROWN, Bruce, E.; 1684 North Sage Hen Road, Orem, UT 84097 (US). ISRAELSEN, D., Brent; 1426 North Grand View, Provo, UT 84604 (US).

(74) Agents: RAUBVOGEL, Amir, H. et al.; Fenwick & West LLP, Two Palo Alto Square, Palo Alto, CA 94306 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

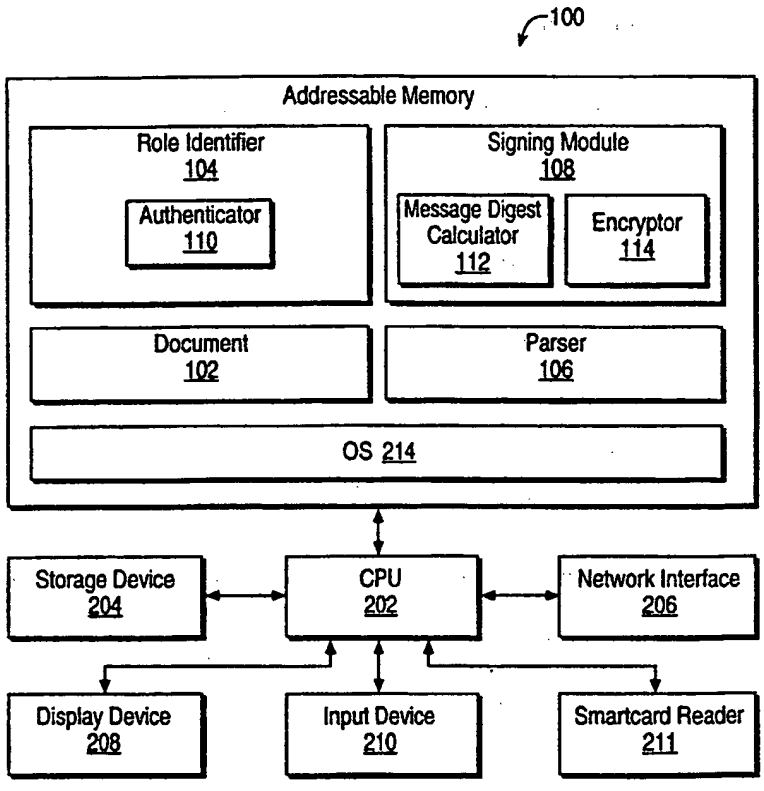
With international search report.

With amended claims and statement.

(54) Title: COLLABORATIVE CREATION, EDITING, REVIEWING, AND SIGNING OF ELECTRONIC DOCUMENTS

(57) Abstract

A virtual signing room facilitates the collaborative creation, editing, reviewing, and signing of electronic documents by parties situated in remote locations. Access to selected parts of documents is provided. The virtual signing room accepts and processes digital signatures coupled with secure authentication of parties to implement document signing. Audit trails and revision tracking are also enabled.



BEST AVAILABLE COPY

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Collaborative Creation, Editing, Reviewing, and Signing of Electronic Documents

Cross-Reference to Related Applications

Background of the Invention

Field of the Invention

The present invention relates generally to electronic documents, and more particularly, to an Internet facility for the collaborative creation, editing, reviewing and signing of electronic documents.

Identification of Copyright

A portion of the disclosure of this patent document contains material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

Description of the Background Art

E-commerce, and more recently e-business, is rapidly becoming the watchword for businesses in this millennium. The appeal of a completely paperless transaction is obvious—reduced storage costs; instant global access to transaction data; the creation of an audit trail; lower transaction costs and the merging, filtering, and

mining of data. Not only will businesses benefit from paperless transactions, but also a number of other institutions, such as courts, financial institutions and government agencies.

A few problems need to be addressed, however, before widespread acceptance of paperless transactions is possible. First, there is a need for an Internet facility or "virtual space" that enables multiple users to share, edit and review documents, wherein each user may be located at different geographical locations. Second, there is a need for a virtual "signing room" that enables real-time access to each of the documents that must be signed to complete a transaction. Finally, there is need to monitor and store actions performed on the documents in order to monitor the transaction for completeness and later legal review.

The problem of enabling multiple users to share, review and edit documents is a key problem for establishing a forum for creating binding legal relationships between geographically diverse entities. For example, a company in Utah may wish to receive funding from several venture capitalist firms in California, Florida and New York. As these agreements are often hotly contested, the ability to review the edits of each of the other parties involved in the transaction, as well as the ability to further modify the documents to bring them in line with expectations, is an essential requirement. In order to avoid the creation of conflicting documents in most transactions today, there is often a lead party that may attempt to represent these diverse interests and serves as the document "holder". The document is often e-mailed to each party whenever any revisions are made in spite of the fact that not every party may be affected by or interested in the revisions. More importantly, the lead party

may not accurately represent the interests of the junior parties; longer delays may thus result due to individual edits performed by each party separately, each of which must then be reviewed separately by each of the other parties and their respective legal counsel. By the time each party's counsel gets an opportunity to review the document, another party in the transaction may have revised the document. The traditional way to avoid these difficulties is to simply assemble all of the parties together in a physical meeting room at a single geographical location. Such an approach may be unfeasible or expensive (due to time and travel cost), and may even result in termination of the deal as a result of the excessive burdens associated with imposing such meetings on all parties involved.

A second problem associated with conventional methods for transacting business is the difficulty in reviewing and agreeing to each of the deal documents involved in the transaction in a timely manner. In a corporate acquisition, for example, there are often several separate agreements that may impact an executive of a company being acquired. The agreements may include a stock transfer agreement, an assignment of intellectual property, an employment agreement and the primary acquisition agreement. Each of these agreements must be signed before the deal is complete. It is standard practice today to fly each of the interested parties out to a single geographical location and to use multiple legal assistants to track down each party and await the review and signature of each party. This process is time-consuming, as each party that signs the agreement must review the agreement and, since several parties are often required to sign the same agreement, each must have individual possession of the agreement during review. Additional problems ensue

when last minute revisions are made to the document prior to a public announcement resulting in a frantic signing session.

This process can also result in errors and/or omissions in the signed documents. A required party may not be available at the time of the meeting. The wrong party may inadvertently sign a document, or the wrong version of a document may be signed by one or more of the parties.

In addition, since each party may need to sign off on a separate set of documents, it is often difficult to ascertain whether all of the required signatures have been properly captured on the correct versions of the documents. In order to minimize such errors, and in order to ensure that each of the agreements has been properly executed, a time-consuming and expensive audit of the agreements is often performed.

What is needed, then, is a system and method for creating a virtual signing room that enables parties to review and edit multiple agreement documents without requiring that the parties be physically present at the same location. What is further needed is a system and method for enabling different individuals to review and sign each of the agreements pertaining to their role in the transaction. What is further needed is a document processing system that provides an audit trail for the signing room that confirms that each party has signed the necessary documents and records each signature accordingly for later verification. Finally, what is needed is a system and method for enabling multiple parties to review, modify, and execute multiple agreements, that minimizes the above limitations and problems of the prior art, reduces costs and burdens, and improves accuracy.

Summary of the Invention

The present invention solves the foregoing problems by providing a virtual signing room that provides real-time access to agreement documents, regardless of geographical locations of the various parties involved, and provides a complete audit trail for all activity occurring in the virtual signing room. The present invention provides quick and easy access to all documents to be reviewed and/or signed by each party, as identified by each party's respective role, and also ensures that documents are signed in the proper order as defined by various commercial standards or other requirements. In a preferred embodiment, the virtual signing room of the present invention advantageously uses document-driven processing of digitally signed, electronic documents, as disclosed in co-pending U.S. Patent Application Serial No. 09/335,443, to help achieve the above-listed objectives.

In one aspect of the invention, a virtual signing room is provided that provides real-time access to agreement documents. In one embodiment, the signing room is a private room that can only be accessed by specified individuals, such as the parties to the transaction. The system uses standard authentication technology, such as digital certificates or biometric devices, to verify a party's identity prior to transmission of the web page or other physical manifestation of the signing room. In one embodiment, the invention includes a signing role identifier for associating the identity of the party with one or more signing roles, a document management system for retrieving each of the necessary documents and providing access to the

documents accordingly, and a deal management module for ensuring that the proper signing sequence is followed and that each of the necessary signatures is received.

In another aspect of the invention, the document management system includes a document privilege module that defines privileges for each of the parties, such as permission levels for viewing, editing and modifying the document or specified portions of the document.

In another aspect of the invention, the document management system includes a notification module for notifying various parties of revisions to one or more of the documents. Such notification may be provided, for example, upon entry into the virtual signing room (e.g. by display of a dialog box, or an on-screen indicator displayed adjacent to recently-modified documents), and/or it may include an e-mail notification to the party. Thus, for example, a party may be notified by e-mail when portions of the documents identified as critical, such as portions affecting price or term of the agreement, are modified but may only be notified upon entry into the virtual signing room when less critical terms are modified. The party may designate which forms of notification are desired for various types of document modifications.

In another aspect of the invention, the document management module includes a document revision list that provides a complete record of the transaction. This might include, for example, a listing of each of the revisions made to the document, the date and time of each revision, and the authenticated party responsible for the revisions. This information could be used during negotiations over the agree-

ment itself or could be used after the fact to help define the parties' intent at the time of the transaction.

In another aspect of the invention, a deal management module is provided that manages the steps associated with completing the deal and monitoring the performance of each of the parties to the deal. In one embodiment, the deal management module includes a list of items that must be accomplished to complete the transaction. In the simplest case, this list might include, for example, a requirement that the entry of contact information into a field of the document is completed and the signature of a party is applied. In a more complex deal, the list might include the requirements that several different agreements are signed at various times (and in a particular order) during the transaction. For example, the deal may be initiated with the application of the signature to a non-disclosure agreement and end with application of the signature to the final acquisition agreement. Furthermore, revisions in the agreements can be used to trigger new items on the list as necessary to effectively complete the transaction.

Brief Description of the Drawings

Figure 1 is a functional block diagram of a system for digitally signing an electronic document according to one embodiment of the present invention.

Figure 2 is a physical block diagram of a system for digitally signing an electronic document according to one embodiment of the present invention.

Figure 3A is a block diagram of an Internet facility for reviewing, editing and signing electronic documents according to one embodiment of the present invention.

Figure 3B is a block diagram showing a four-tier architecture for implementing one embodiment of the present invention.

Figure 3C is a block diagram showing a four-tier architecture including an E-Cabinet for implementing one embodiment of the present invention.

Figures 4A-4B are screenshots of a sample system for digitally signing an electronic document according to one embodiment of the present invention.

Figures 5A-5B depict an example of an agreement document in paper form.

Figures 6A-6B depict an example of a screen display of an agreement document.

Figure 7A is a flowchart illustrating the process of entering a virtual signing room according to one embodiment of the present invention.

Figure 7B is a flowchart illustrating the process of reviewing and signing a document according to one embodiment of the present invention.

Figures 8A-8B depict an example of a screen display of a completed and digitally signed agreement document.

Figure 9 is an example of a screen display of an ACH Authorization Form.

Figures 10A-10B depict an example of a screen display for a Change and Enrollment Form.

Figure 11 is an example of a screen display for passphrase entry and key generation.

Figure 12 is an example of a screen display for private key retrieval.

Figure 13 is a flowchart showing a document signing method according to one embodiment of the present invention.

Figure 14 is a system block diagram of one embodiment of a document management flow process in a signing room implemented according to the present invention.

Figure 15 is a system block diagram of one embodiment of a document management flow process in a disclosure room implemented according to the present invention.

Figure 16A is a flowchart showing a signing room logon and entry method according to one embodiment of the present invention.

Figure 16B is a flowchart showing a signing room admittance procedure according to one embodiment of the present invention.

Figure 16C is a flowchart showing an account termination method according to one embodiment of the present invention.

Figure 17 is a flowchart showing an example of an electronic signature collection method according to one embodiment of the present invention.

Figures 18A-D are screen shots showing an example of a signing room according to one embodiment of the present invention.

Figure 19 is a flowchart showing a deed recording method according to one embodiment of the present invention.

Figure 20 is a block diagram showing a mortgage signing room architecture according to one embodiment of the present invention.

Figure 21 is a site architecture diagram of a mortgage signing room according to one embodiment of the present invention.

Detailed Description of the Preferred Embodiments

A preferred embodiment of the invention is now described with reference to the Figures, where like reference numbers indicate identical or functionally similar elements. The particular sequence of steps shown in the various methods described below may be performed, for example, by a computer or set of computers following a set of instructions specified in software code. One skilled in the art will recognize that other mechanisms and implementations for performing such methods may also be employed.

Referring now to Figure 1, there is shown a functional block diagram of a system 100 for digitally signing electronic documents 102. Although this system will be used to describe one embodiment of the present invention, other document processing systems could also be used to implement the virtual signing room. As described hereafter, each document 102 is preferably encoded using a markup language, such as the February 1998 W3C Recommendation Extensible Markup Language (XML) 1.0, although the invention is not limited in that respect. For example, the standard generalized markup language (SGML, ISO 8879) or another markup language could be used without departing from the spirit of the invention. Preferably, the document 102 is indexed for full text searching, and the document data within tagged fields are indexed for field searches. The indexing allows a user to easily perform document queries using techniques well known to those skilled in the art.

The document 102 may represent any of a number of legal or commercial instruments, such as sales contracts, licenses, non-disclosure agreements, patent applications, court pleadings, mortgages, and the like. Appendix A is an example of a

document type definition (DTD) in the context of an electronic court filing system. Appendices B and C show an example of an XML-encoded document corresponding to the agreement document depicted in Figures 6A-6B. Appendix B shows the document in its initial state; Appendix C shows the document after it has been completed and digitally signed. It should be recognized that a wide variety of applications, instruments, and/or document types may be provided within the scope of the present invention.

Briefly, the principal components of the system 100 include a role identifier 104, a parser 106, and a signing module 108. In one embodiment, the foregoing components are implemented as software modules running on a conventional personal computer employing, for example the Microsoft® Windows 98 operating system and an Intel® Pentium microprocessor, although other implementations are possible. For example, the components could be distributed among a plurality of computers within a network. Alternatively, the components could be implemented as hardware devices within an embedded system. Although the components are described herein as separate functional units, those skilled in the art will recognize that various components may be combined or integrated into a single software application or device.

The role identifier 104 determines the role or capacity in which a signer is to digitally sign the electronic document 102. Unlike conventional systems which are limited to the signing of an entire document by a single person in a single role or capacity, the present invention allows multiple individuals to sign different portions of the document 102 in multiple different roles or capacities. Thus, the present invention enables the signing of complex, real-world documents.

In one embodiment, the role identifier 104 is implemented as a Web browser, such as the Microsoft Internet Explorer, available from Microsoft Corporation of Redmond, Washington. Preferably, the role identifier 104 receives input from the signer to determine the signer's identity and/or role. As discussed in greater detail below, the input is obtained using conventional input mechanisms such as pull-down menus, radio buttons, text entry boxes, and the like.

In one embodiment, the role identifier 104 includes an authenticator 110, which is used to authenticate the signer's identity, as well as the signer's authorization to sign the document 102 in the specified role. Although a variety of authentication systems exist, a public key cryptosystem is preferably used to authenticate the signer, as described hereafter. In one embodiment, the authenticator 110 is implemented as a "plug-in" module to a conventional Web browser. Although the authenticator 110 is illustrated herein as a component of the role identifier 104, it should be recognized that the authenticator 110 could be implemented as a separate functional unit.

Coupled to the role identifier 104, the parser 106 parses the document 102 to identify the portion to be signed by the signer, i.e. the "to-be-signed" portion. In one embodiment, the parser 106 is an XML parser adapted to parse an XML-encoded document 102. As described in greater detail below, the parser 106 identifies within the document 102 a "to-be-signed" tag 116 or other delimiter for indicating a portion of the document 102 to be signed by the signer in the specified role or capacity. The document 102 may include a plurality of such tags 116 corresponding to the plurality of signers and roles. In addition, the parser 106 may be used to identify one or

more "accessible-by" tags 120 within the document 120, as described in greater detail hereafter.

In a preferred embodiment, XML is used because it may be parsed using a relatively simple parser 106. However, as noted above, SGML or another markup language could be used without departing from the spirit of the invention. In one embodiment, the parser 106 is a commercially available XML parser, such as the XML parser available from Microsoft Corporation. However, a custom-designed parser 106 could also be used within the scope of the present invention.

Coupled to the parser 106, the signing module 108 applies the signer's digital signature to the identified to-be-signed portion of the document 102. In one embodiment, the signing module 108 applies the digital signature using the RSA Public Key Cryptosystem, available from RSA Data Security, Inc. of San Mateo, California, although the invention is not limited in that respect. The RSA Public Key Cryptosystem is well known to those skilled in the art, and has become a de facto standard for cryptographic communications and digital signatures. In one embodiment, the signing module 108 is implemented as a "plug-in" module to a standard Web browser, although other implementations are possible without departing from the spirit of the invention.

In one embodiment, the signing module 108 includes a message digest calculator 112 for calculating a message digest for the to-be-signed portion. As noted above, the message digest is a number or code that represents the to-be-signed portion of the document 102. Preferably, the message digest is calculated using a one-way hash function, such as the Secure Hash Algorithm (SHA) or Message Digest

(MD5), whereby any change to the message will result in a different calculated message digest. SHA was developed by NIST as specified in the SHS (Secure Hash Standard). The algorithm takes a message (less than 2^{64} bits of length) and produces a 160-bit message digest. MD5 was developed by RSA and takes a message of arbitrary length and produces a 128-bit message digest. Although the message digest calculator 112 is illustrated herein as a component of the signing module 108, it should be recognized that the calculator 112 could be implemented as a separate functional unit.

The signing module 108 also includes an encryptor 114 for encrypting the message digest with the signer's private key. The encrypted message digest is referred to herein as a digital signature 118. In one embodiment, the digital signature 118 is stored within the document 102 and associated with the portion of the document 102 that was signed. Alternatively, the digital signature may be stored with other document audit information for later verification. Although the encryptor 114 is illustrated herein as a component of the signing module 108, it should be recognized that the encryptor 114 could be implemented as a separate functional unit.

Referring now to Figure 2, there is shown a physical block diagram showing the components used to implement the functionality of Figure 1, according to one embodiment of the present invention. A central processing unit (CPU) 202 executes software instructions and interacts with other system components to perform the methods of the present invention. A storage device 204, coupled to the CPU 202, provides long-term storage of data and software programs, and may be imple-

mented as a hard disk drive or other suitable mass storage device. In one embodiment, the storage device 204 stores a plurality of documents 102 to be signed.

A network interface 206, coupled to the CPU 202, connects the system 100 to a network (not shown), such as the Internet. Such connection is implemented according to techniques that are known in the art. A display device 208, coupled to the CPU 202, displays text and graphics under the control of the CPU 202. An input device 210, coupled to the CPU 202, such as a mouse or keyboard, facilities user control of the system 100. A "smartcard" reader 211, coupled to the CPU 202, facilitates access to a smartcard for authentication purposes, as described in greater detail below.

An addressable memory 212, coupled to the CPU 202, stores software instructions to be executed by the CPU 202, and is implemented using a combination of standard memory devices, such as random access memory (RAM) and read-only memory (ROM) devices. In one embodiment, the memory 212 stores the above-described document 102 and software modules, including the role identifier 104, parser 106, signing module 108, authenticator 110, message digest calculator 112, and encryptor 114.

In one embodiment, the memory 212 also includes an operating system 214 for managing and providing system resources to the above-mentioned software modules. Preferably, Windows 98, available from Microsoft Corporation, is used, although a variety of other operating systems 228, such as Windows 2000, MacOS 8, UNIX, or Linux may be used within the scope of the present invention.

Referring now to Figure 3A, there is shown a block diagram that illustrates one embodiment of an Internet facility for reviewing, editing and signing electronic documents according to the present invention. In one embodiment, the invention includes a

virtual signing room 300 implemented as a web page using XML technology. Alternatively, other markup languages could be used. The signing room 300 comprises three separate logical modules: a document management module 310; a party-to-document mapping module 320; and a deal management module 330.

The document management module 310 serves to manage the documents associated with the deal or transaction. Module 310 also monitors and maintains an audit trail for any revisions or alterations made to the documents. In one embodiment, the document management module 310 establishes access rules for determining to what extent each party in the deal room has permission to view and/or modify each document. Once a party is authenticated and enters the signing room, the document management module 310 retrieves the documents that the party has permission to view by making calls to the document-to-party mapping module 320. As described above, for each document, permissions may be granted for the entire document or for a portion of the document associated with the authenticated party. Furthermore, the document management module 310 determines whether any revision privileges exist for the party with respect to retrieved documents. Again, such privileges may be defined with respect to an entire document or may only apply to a portion of the document. For example, one party may have the ability to modify the correspondence address used in the agreement or the spelling of their own name but may not be permitted to make any revisions to other material terms in the agreement.

In one embodiment, the document management module 310 includes an audit module 315. The audit module 315 tracks and stores all revisions 318 to the documents made by each party. By storing the revisions 318 to the documents, the audit module

provides a roadmap beginning with the initial version 316 of the agreement and ending with the final version incorporating revisions 318, thereby enabling better interpretation of the resulting agreement by the parties. Furthermore, the functionality of the audit module 315 can be used in conjunction with a notification module 317 to provide notification to the parties of any revisions to the documents.

In one embodiment of the invention, the notification module 317 may be used to notify different parties of revisions to one or more of the documents. Such notification may be provided, for example, upon entry into the virtual signing room 300 (e.g. by display of a dialog box, or an on-screen indicator displayed adjacent to recently-modified documents), and/or it may include an e-mail notification to the party. Thus, for example, a party may be notified by e-mail when portions of the documents identified as critical, such as portions affecting price or term of the agreement, are modified but may only be notified upon entry into the virtual signing room when less critical terms are modified. In one embodiment, the party may designate which forms of notification are desired for various types of document modifications.

In one embodiment, the party-to-document mapping module 320 includes a role identifier 104 for generating and maintaining a map 322 assigning a role for each party, and a map 324 for associating each role with one or more documents. As noted earlier, the role identifier 104 receives input from the signer to determine the signer's identity and/or role. In one embodiment, the role identifier 104 uses conventional input mechanisms such as pull-down menus, radio buttons, or text entry boxes to receive input specifying a role. The present invention thus facilitates man-

agement of document privileges in the context of a complex transaction where each party may be associated with multiple roles. For example, an executive in a company may serve as a board member, a shareholder, an employee and an inventor. By providing access to documents based on a role, the executive can review each agreement separately by selecting each role in turn. Alternatively, the party may wish to simply receive all documents that are associated with each of the roles that the party has been assigned.

For example, in one embodiment as illustrated in Figures 4A and 4B, the signer's role is specified by means of a pull-down menu 402. Likewise, in certain embodiments, the identity of the signer may be obtained from a "cookie" or from network login information. However, it should be recognized that the signer's identity could be separately specified.

Once a role has been specified, the party-to-document mapping module 320 retrieves a list 404 of possible documents 102 to be signed by the party. For example, as shown in Figure 4A, the selection of the role of "Governor" from the pull-down menu 402 results in a list 404 of bills to be signed by the Governor. Likewise, as shown in Figure 4B, the selection of "Clerk" from the menu 402 results in a list 404 of bills to be reviewed and approved by the Clerk.

While using the party-to-document mapping module 320 in conjunction with a previously generated list is one method for determining the documents to be signed by a party, the list 404 may be generated dynamically in a number of ways. For example, as described more fully hereafter, the parser 106 may parse a plurality of documents 102 (located either in the storage device 204 or in memory 212) to iden-

tify each to-be-signed tag 116 contained therein. As noted earlier, each to-be-signed tag 116 indicates a role of a signer. Thus, an index (not shown) of documents 102 and roles may be created, which may then be used by the role identifier 104 to generate a list 404 of documents 102 for a specific role. This enables the addition of documents at a later time without requiring an administrator to recreate a new list with each new document.

A deal management module 330 is also provided for managing a deal completion list 332 of items that must be accomplished to complete the deal. In the simplest case, this list might include, for example, a requirement that certain contact information be entered in a field of the document and that a signature be applied, or that two signatures be applied to a document in a particular order. In a more complex deal, the list might include, for example, application of one or more signatures to several different agreements at various times during the agreement. For example, the deal may be initiated with application of a signature to a non-disclosure agreement and end with application of a signature to a final acquisition agreement.

In one embodiment, a next step module 334 is provided that monitors and attempts to complete the next step in the deal. This might involve, for example, automatically sending an e-mail message to the party that is responsible for the next step in the deal. Alternatively, the next step at a given stage of the deal may involve, for example, retrieving a document from another server or generating a summary of the agreement; the next step module 334 interactively makes requests as necessary to complete the appropriate task.

Additionally, the deal management module 330 may add new items to the list responsive to revisions in one or more of the agreements in order to effectively complete the new transaction. The application of a signature to a project agreement, for example, may dictate that a project description be added to the list to complete the transaction.

Referring now to Figure 3B, there is shown a four-tier architecture as may be used for implementing one embodiment of the present invention. The four tiers include, for example:

- Client tier 341, such as a conventional browser;
- Presentation tier 341, including functionality for authentication, signing room, E-Cabinet, and administration, as described in more detail below;
- Business logic tier 343, including functionality, such as a Virtual File Clerk (described in more detail below) for processing requests and performing other business functions; and
- Persistent storage tier 344, including database (RDBMS) and document store.

Tiers interact with one another to perform the functionality of the network-based application, as is known in the art. In one embodiment, the virtual signing room of the present invention is implemented as part of presentation tier 341, along with other functionality.

Referring now to Figure 3C, there is shown a block diagram illustrating the functional modules of presentation tier 342, including authentication 352, signing

room 300, and E-Cabinet 352. E-Cabinet 352 is a presentation-level tier application that provides access to a repository of documents, such as may be stored in persistent storage tier 344 (on a database, for example). E-Cabinet 352 may be used, for example, to archive documents after completion of a deal or other transaction. Access to particular documents within E-Cabinet 352 may be permitted or restricted based on various characteristics, subject to verification of the user's identity.

Thus, for example, a user would provide a user name, password, and/or additional identity verification such as digital signature and biometrics. The user then selects a role from a list of available roles in connection with E-Cabinet 352. E-Cabinet 352 presents the user, via a browser, with a list of documents that are relevant to the user and his or her selected role.

In one embodiment, various views and modes of accessing documents may be provided, including a search function 353, status report 354 as to selected documents, and hierarchical display 355 of documents. Search function 353 may provide, for example, full text indexing and searching, and/or field-specific search functionality for documents in the E-Cabinet 352 (which are stored in persistent storage tier 344 such as a database). Business logic tier 343, such as a virtual file clerk, processes requests made by the user, retrieves the appropriate data from persistent storage tier 344, filters the results so that they only contain information to which the user has access, and provides the documents for display in client tier 341.

One skilled in the art will recognize that the architecture shown in Figures 3B and 3C, and the E-Cabinet functionality described above, are merely exemplary, and

that other architectures and methods for implementing the present invention are possible.

Referring now to Figure 7A, there is shown a flowchart illustrating the process of entering the virtual signing room 300. As an initial matter, the identity of the party attempting to enter the Internet facility or signing room 300 is requested 702. This might involve user entry of a user name with a password that can be issued to log into all deals pending on that server or might involve entering a special code that has been provided to the party for a single deal.

The method continues by authenticating 704 the party for the specified role. The authenticator 110 verifies the identity of the party before the party is allowed to sign the document 102 in the specified role or capacity. If the authentication is unsuccessful, the invention detects and prevents the unauthorized access.

Various forms of authentication may be performed in connection with the present invention. For example, public key cryptography offers a particularly secure method for authentication. In one embodiment, the party inserts a smartcard encoded with his or her private key into the smartcard reader 211. Smartcards and smartcard readers 211 are available from a variety of sources, such as Micromodular Data Solutions of Santa Clara, California.

The authenticator 110 uses the private key encoded within the smartcard to encrypt a standard message. Thereafter, the authenticator 110 attempts to decrypt the message using the party's public key, which may be obtained from a public key database or the like using a standard protocol, such as the Lightweight Directory Access Protocol (LDAP), which is part of the X.500 standards. If the message is suc-

cessfully decrypted, the smartcard is known to contain the private key of the authorized signer.

For even greater security, the smartcard may contain previously-acquired biometric data of the signer, such as digitized fingerprints, voiceprints, facial configurations, iris images, and the like, which may be compared with new biometric data obtained at the time of authentication using a biometric data acquisition device (not shown). Biometric data acquisition devices are well known in the art and may be obtained from a variety of sources. For example, fingerprint identification systems may be obtained from Digital Persona, of Redwood City, California. Likewise, SAFlink Corp., of Tampa, Florida provides a system for voice, face and fingerprint recognition. IriScan, Inc. of Marlton, New Jersey provides a system for iris scanning.

If the previously acquired data substantially matches the new biometric data (within acceptable tolerances for noise and other effects), the party will be declared authentic. In combination with the public key authentication system discussed above, the foregoing technique makes the signer's digital signature far more reliable and difficult to repudiate than its handwritten equivalent.

In alternative embodiments requiring a lesser degree of security, the party may provide a pass phrase or the like to the role identifier 104, after which the pass phrase is compared against a database of pass phrases for various signing roles. If a match is found, the party is authorized for the corresponding role and is allowed to enter the signing room 300.

Referring now to Figure 7B, there is shown a flow chart illustrating the process of reviewing and signing a document. The method begins by obtaining 706 the

private key of the signer. As noted earlier, the private key is used for generating the signer's digital signature 118. In the smartcard embodiment described above, the signer's private key is retrieved from the smartcard. Various security measures, well known to those skilled in the art, may be used to prevent unauthorized access to and retrieval of the signer's private key. In the case of the pass phrase embodiment, a private key is preferably stored within the database for each pass phrase. When a match is found, the corresponding private key is retrieved from the database.

After the private key is obtained, the method continues by locating 708 a to-be-signed tag 116 within the document 102 corresponding to the specified role of the signer. As explained above, the to-be-signed tag 116 is an XML tag used for indicating a portion of the document 102 to be signed. In an alternative embodiment, an XML attribute is used for the same purpose. The parser 106 parses the document 102 to find the to-be-signed tag 116 corresponding to the specified role. If the parser 106 is unable to find the tag 116, an error is preferably generated.

Thereafter, the to-be-signed tag 116 is used to identify 710 the to-be-signed portion of the document corresponding to the role of the signer. In one embodiment, each to-be-signed tag 116 comprises a beginning tag (comprising an identification of a role) and an end tag. For example, a to-be-signed tag 116 has the following form in one embodiment:

```
<TBSigned SigID=''Governor''>
. . .
</TBSigned>
```

The text between the beginning tag and end tag is the to-be-signed portion of the document 102. The use of to-be-signed tags 116 allows various portions of a

document 102 to be signed by different individuals, unlike some conventional systems that are limited to signing an entire document by a single individual.

After the to-be-signed portion is identified, a check 712 is made whether access to any portion of the document 102 is restricted, indicating that the portion should not be displayed to the signer. The ability to restrict the viewing of particular portions of a document 102 is advantageous in many contexts. For example, an electronically filed court document might include portions that are sealed by a court order, while the unsealed portions should still be available to be viewed by the public. Similarly, certain agreements may include portions that are not relevant to certain individuals, and thus should not be viewed by particular signers. Thus, in one embodiment, access restrictions may be placed on the document 102 in order to allow the signer to view certain portions and not others. This is an advance over conventional systems in which a digitally signed word-processing or otherwise-encoded document must be displayed to the signer in its entirety or not at all.

As described above, the document 102 may include one or more accessible-by tags 120 for indicating access restrictions to portions of the document 102. In an alternative embodiment, XML attributes are used for the same purpose. Like the to-be-signed tag 116, the accessible-by tag 120 includes a beginning tag and an end tag, and the text between the tags is the portion of the document 102 that is access-restricted. Preferably, the parser 106 is used to identify the access-restricted portions of the document 102.

In one embodiment, the accessible-by tag 120 includes an indication of one or more roles, access levels, or the like, of individuals who may view the document 102. For example, in one embodiment, an accessible-by tag 120 has the following format:

```
<AccessibleBy>
<ViewModify><PersInfo Role=''Judge''></ViewModify>
<View><PersInfo Role=''Plaintiff''></View>
. . .
</AccessibleBy>
```

In this example, the judge may both view and modify the document 102, while the plaintiff may only view the document 102. Preferably, all other individuals would not be able to view or modify the document.

If, in step 712, it is determined that the document includes access restrictions, the method continues with step 714 by preventing unauthorized access to the access-restricted portions, such as by masking the display of, and/or preventing revisions or modifications to, those portions. In one embodiment, one or more masked portions may be encrypted using the public key of the person authorized to access those portions. As a result, if the signer is the authorized party, only she may use her private key to decrypt and display the masked portions.

After either steps 712 or 714, the method continues by displaying 716 the document 102, excluding any masked portions, to the signer, and accepting any edits or revisions to the portions accessible to the signer. This allows the signer to review the document 102 and make any required selections or revisions before applying his or her digital signature 118.

After the document 102 has been displayed and edited, the method continues by receiving 718 from the signer an indication to sign the document 102. This may be accomplished in any of a variety of ways, as will be apparent to one skilled in the art. For example, the signer may use the input device 210 to click on a "sign now" button or the like.

Next, the method continues by storing 720 in the to-be-signed portion of the document 102 the date and time at which the document 102 is signed. Preferably, the current date and time is read from a system clock (not shown) or the like, which is coupled to the CPU 202. The inclusion of a time and date stamp is useful for auditing purposes, and for later verification of the validity and applicability of the signed document 102, for example in a court or administrative proceeding. By providing date and time stamps for individually-signed portions of the documents 102, the present invention provides advantages over conventional systems which may not be able to realistically model documents 102 that are signed at different dates and times by different individuals.

In one embodiment, date and time tags are added to the to-be-signed portion, identifying the date and time at which the signer signs the document 102. For example, the date and time tags have the following format in one embodiment:

```
<date>01-02-1999</date>
<time>15:43:16.12</time>
```

By adding the date and time tags to the to-be-signed portion, the tags are digitally signed, so that the signer cannot later repudiate the date and time of the digital signature.

After the date and time are stored, the method continues by calculating a message digest for the to-be-signed portion of the document 102. As noted above, this is accomplished in one embodiment using a one-way hash function, such as SHA or MD5, whereby any change to the message will result in a different calculated message digest. Those skilled in the art will recognize that a variety of other hash functions could be used without departing from the spirit of the invention.

Thereafter, the method continues by encrypting 722 the message digest using the signer's private key to generate the signer's digital signature 118. While it is possible to encrypt the whole document 102 without departing from the spirit or essential characteristics of the present invention, it is typically not necessary to do so, because many documents are non-private except for specific portions that may be masked as described above. Moreover, since encrypting a document (such as by public key cryptography, symmetric cryptography, or other means) can be relatively slow, it is advantageous to minimize the amount of data encrypted.

After the digital signature 118 is created, the method continues by storing the digital signature 118 within the document 102. In one embodiment, the digital signature 118 is stored directly after the to-be-signed portion, although one skilled in the art will recognize that the signature 118 can be stored at other locations.

In one embodiment, the document 102 includes a signing history portion for storing the digital signature 118 of each signer of the document 102. The signing history portion may be separately designated by an XML tag, such as `<Signatures></Signatures>`, and forms a convenient location for storage of information indicating which signers have signed the document 102.

After the digital signature 118 is stored, the method continues by obtaining 728 and storing the signer's digital certificate. A digital certificate is an attachment to a document 102 that provides additional verification that the signer is whom he or she claims to be. An individual wishing to digitally sign a document applies for a digital certificate from a Certificate Authority (CA), such as Verisign, Inc., of Mountain View, California. The CA issues an encrypted digital certificate containing the individual's public key and a variety of other identification information. The CA makes its own public key readily available, such as through print publicity and/or via the Internet. Thus, the recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the document 102, verifies it is issued by the CA, and then obtains the sender's public key and identification information held within the certificate. The recipient thus obtains some assurance that the signer is whom he or she claims to be. In one embodiment, the ANSI X.509 standard is used for such digital certificates in connection with the present invention.

In one embodiment, the signer's digital certificate is obtained from the signer's smartcard, as discussed above. In alternative embodiments, the certificate may be obtained from a database after the signer is authenticated with a pass phrase or the like. The digital certificate is preferably stored in the document 102 near the associated digital signature 118. In one embodiment, the digital certificate is identified within the document 102 by a `<Cert></Cert>` tag.

After the digital certificate is stored, the method continues by displaying 730 a visual indication of the signer's digital signature 118 in conjunction with the display of the document 102. Any of a variety of techniques may be employed. For example,

a digitized version of the signer's handwritten signature (not shown) may be applied to the document 102. Likewise, in appropriate situations, a graphical seal (not shown) could be displayed. This may be particularly appropriate, for example, in the case of a "digital notary", who may perform a similar function as a notary public by verifying a signer's digital signature and digital certificate with a CA. Moreover, an ASCII or Base 64 representation (not shown) of the digital signature 118 could also be displayed. Other representations and indications are also possible, such as graphical overlays and the like. After the visual indication is displayed, the method of Figure 7B is complete.

The present invention also facilitates collaborative document editing by remote-located parties. Previously stored revision privileges associated with a party are retrieved, and revisions are permitted according to the level of privileges. In some situations, a party may only have rights to modify a portion of the document. Any number of conventional locking mechanisms may be employed to prevent modifications or revisions to document data. For example, text fields may be marked with "read only" attributes, and text entry fields, pull down menus, and radio buttons may be "grayed out" to prevent modifications to the document 102 using techniques well known to those skilled in the art.

If a party wishes to modify the document, the audit module 315 may be initiated to track the revisions and to record the party's identity accordingly. Additionally, as described above with reference to Figure 3A, the audit module 315 verifies whether any notifications should be transmitted to one or more of the other parties to the agreement. If so, the audit module 315 performs the action associated with the

type of revision. For example, if a field has been tagged as "critical", then an e-mail message may be immediately transmitted to one of the parties.

Referring now to Figure 20, there is shown a block diagram depicting a mortgage signing room architecture according to one embodiment of the present invention. For illustrative purposes, the block diagram of Figure 20 shows the various parties and components that may interact with one embodiment of the present invention to implement a mortgage-related transaction. As can be seen from the Figure, signing room 300 forms a central location for access to and modification of various documents, including for example, documents to be recorded 2102, title insurance 2104, mortgage closing documents 2108, certificate validations 2109, appraisals and certificates 2111, and notarizations 2112. Signing room 300 also provides a mechanism for initiating and managing electronic fund transfers 2110, such as between a party and a bank 2008, as described in more detail below.

Various parties interact with the signing room 300 to create, modify, and/or sign any or all of the above documents, or to supply support services. Such parties include, for example, a county recorder 2002, title company 2004, mortgage company 2006, digital certificate authority 2007, bank 2008, appraisers and inspectors 2009, and notaries 2010. Additional parties involved in the transaction, such as the county assessor 2001, the Internal Revenue Service 2003, lender 2005, and the like, may also interact with signing room 300 or may instead interact with other parties in a conventional manner, in connection with, for example, tax assessments and liens 2101, federal tax liens 2103, loan documents 2107, and signed loan documents 2106. The title company 2004 and county recorder 2002 may also share research 2105, if de-

sired. One skilled in the art will recognize that many other parties, interactions, and documents may be associated with or connected with a transaction implemented by the present invention.

In one embodiment, key parties to the transaction, such as a buyer's real estate agent and/or attorneys 2104, borrower 2105, and seller's real estate agent and/or attorneys 2106, access signing room 300 via a "portal" website 2011 over the Internet 2012. A conventional browser may be used for such interaction with the system of the present invention. Additional parties, such as the buyer 2013 and the seller 2017, may also interact with the present invention, or may be represented by parties 2014 and 2016.

Referring now to Figure 21, there is shown a site architecture for a mortgage signing room 300 according to one embodiment of the present invention. The site architecture of Figure 21 may be implemented, for example in a web site as may be accessible over the Internet. Signing room 300 contains several sections and areas for implementing the systems and methods of the present invention, including for example:

- Administration 2201: Includes functionality for setting up an account, identifying parties and roles, defining workflow, and transferring in documents;
- Editing 2202: Includes functionality for opening documents, creating virtual copies of documents, making revisions and changes, and initiating new versions;

- Verify 2203: Includes functionality for identifying documents to be verified, checking certificates and a Certificate Revocation List (CRL), and verifying by public key;
- Closing 2204: Includes functionality for monitoring application of signatures to documents, advising parties of the next requirements in the transaction, verifying signatures as documents are signed (in conjunction with verify 2203 area), transmitting deeds and mortgage to county recorder, sending documents to all relevant parties, disbursing funds, and archiving communications to database or CD-ROM;
- Archive 2205: Includes functionality for archiving, verifying, indexing, compressing, retrieving by search, and the like;
- Signature 2206: Includes functionality for presenting unsigned documents by e-mail, identifying the sender, requesting signature, and applying signature;
- Certification 2207: Includes functionality for applying for a digital certificate, selecting a security level and/or strategy, issuing the certificate, filing the security level and/or strategy, and sending the certificate to the party; and
- Notarization 2208: Includes functionality for presenting a document, identifying the party, acknowledging the digital signature and/or notarizing the signature. Such techniques are described, for example, in U.S. Patent No. 5,872,848, for "Method and apparatus for witnessed

authentication of electronic documents," issued February 16, 1999, the disclosure of which is incorporated herein by reference.

Referring now to Figures 5A-5B, there is shown an example of an agreement document 500 in paper form according to the prior art. Various entry fields 501 and signature fields 502 are provided for manual entry of information and signatures. The document is divided into several sections 503-511, each containing various types of information and fields 501 and/or 502. In addition, terms and conditions 512, as well as application instructions 513, are provided, as may appear on the back of the printed copy of document 500.

As can be seen from the example of Figures 5A-5B, some sections of document 500 may not be applicable or relevant to some parties to the agreement, or may be more suitable for completion and/or signing at different times than other sections of document 500. For example, placement information 505 may not be relevant or available at the time the agreement is initially filled in, but may be suitable for later completion when such information is known. Also, such information 505 may be more suitably completed by a different party than the party responsible for completing the other sections of document 500.

One disadvantage of paper forms such as that shown in Figures 5A-5B is that such distributed completion and signing of the document is cumbersome and difficult to implement satisfactorily. For example, the party filling in placement information 505 may see credit card information 508 that has previously been filled in, when such information is not relevant to that party. In addition, particular sections of

terms and conditions 512 may only apply to particular parties, but the paper form does not permit selective "signing off" on such individual sections.

In addition, supplementary forms or other requirements may not easily be provided or associated with the document 500. For example, if an Automated Clearing House (ACH) authorization form is required because a third-party credit card is to be used, such a form may inadvertently be omitted because the party signing document 500 may not be aware of such a requirement, even though paragraph 514 of instructions 513 states that such a supplementary form is required.

Referring now to Figures 6A-6B, there is shown an example of a screen display 600 of an agreement document corresponding to the paper document 500 of Figures 5A and 5B. The screen display 600 may be displayed using a conventional browser as is known in the art. As can be seen from the screen display 600, many of the problems and limitations associated with paper documents are eliminated or minimized. Various fields 601 are provided for entry of information corresponding to fields 501 in document 500. If appropriate, fields 601 only include a subset of fields 501, depending on the particular items of information to be collected from the party viewing the display 600. Thus, for other parties providing other items of information, a different set of fields 601 might be displayed, corresponding to the items of information being sought.

Note buttons 604 are provided for accessing or providing additional information as may be relevant to fields 601 adjacent to buttons 604.

Generate keys button 602 provides access to functionality for generating public and private keys, as described below in connection with Figure 12. Explain button 603 provides additional information regarding the function of button 602.

Enroll button 605 specifies that the party viewing the screen display 600 wishes to enroll in an auto-shipment program. This is an example of an application of the present invention, whereby a button 605 is used to activate a secondary form or agreement (described below in connection with Figures 10A-10B) that is only applicable in certain circumstances. Thus, the additional information to be collected in association with the auto-shipment program can be relegated to the secondary form rather than presented in the primary form. This helps to make the primary form less confusing, as the party need not be concerned with areas on the form that are not applicable to his or her particular situation or specified requests. In the example shown, sections 507 and 508 of the paper document 500 of Fig. 5A can be eliminated from the primary display 600, since they are only applicable if the user clicks on button 605 to specify an interest in the auto-shipment program.

Similarly, checkbox 606 allows the party viewing the screen display 600 to select whether he or she is a nonresident alien. If so, another secondary form (not shown) may be provided to obtain further information on such a situation. Likewise, ACH button 607 provides access to another form for collecting ACH data, as described below in connection with Figure 9Scrolling text box 608 displays the text of the terms and agreement. The party indicates his or her assent to the terms, and asserts the accuracy of the provided information, by clicking on Sign button 609. As

described above, authentication of the signer's identity may be verified by whatever means are appropriate.

Referring now to Figures 8A-8B, there is shown an example of a screen display of a completed and digitally signed agreement document. This screen may be provided, for example, when a user or party wishes to view a previously signed document or agreement. Fields 801 are populated with data as was entered previously in fields 601 of Figures 6A-6B. Note buttons 604 are also provided, enabling access to supplemental information regarding various fields 801. Statement 806 provides an affirmative statement reflecting the party's entry in checkbox 606. Field 802, showing the credit card number of the party, is partially obscured so as to hide sensitive data from the viewer. Depending on the identity of the person viewing screen 800, and the degree to which that identity can be verified, fields such as 802 displaying sensitive data may be omitted, obscured, or displayed in part or in full. Parameters for such display may be specified in advance, if desired.

A hexadecimal representation of the signer's digital signature 803 is provided, giving the viewer of screen 800 some assurance that the digital signature has in fact been obtained. In addition, in the example of Figures 8A-8B, a hexadecimal representation of the certificate 804 corresponding to the signer and verifying his or her identity, is also shown. This certificate 804 provides an additional level of certainty as to the identity of the signer. One skilled in the art will recognize that many other representations of the digital signature and/or certificate may instead be displayed, including for example a simple notification or graphical element.

Referring now to Figure 9, there is shown an example of a screen display of an ACH Authorization Form 900. Form 900 may be displayed, for example, when a party indicates payment by ACH using button 607 of document 600. In this manner, the additional information 901 sought in form 900 is only collected when applicable. In addition, the particular digital signature that is affixed by clicking on button 902 is applicable to the particular fields and text shown in form 900. Thus, the present invention provides a mechanism for digitally signing portions of documents as applicable or appropriate. In one embodiment, upon signing (by clicking on button 902), the party is again presented with document 600 for collection of additional information.

Referring now to Figures 10A-10B, there is shown an example of a screen display for a Change and Enrollment Form 1000. Form 1000 may be displayed, for example, when a party indicates that he or she clicks on button 605 (shown in Figure 6A) to begin the process of enrolling in an "AutoShip" program. One skilled in the art will recognize that form 1000 is merely exemplary of a secondary form that is activated by user selection of an element of a primary form.

Additional information 1001 is collected, and the user may select from various options 1002 for the AutoShip program by clicking on checkboxes. A further option for discontinuing membership in the program is also provided 1003. Payment information is provided in 1004, and the party may digitally sign the document by clicking on button 1005. In one embodiment, upon signing (by clicking on button 902), the party is again presented with document 600 for collection of additional information.

As will be apparent to one skilled in the art, the various primary and secondary forms and agreements can be presented as applicable to any party or combination of parties. Thus, different types of information may be collected from different parties, and some sensitive information may not be displayed to all parties. The present invention facilitates such flexibility of document review, access, and execution.

Referring now to Fig. 11, there is shown a screen display 1100 for passphrase entry and key generation. In one embodiment, the party is presented with screen 1100 after he or she clicks on button 602 (shown in Figure 6A). The party enters a passphrase in input field 1101 and confirms entry in field 1102. Optionally, the party may specify a file name and/or path for a file containing the private key in field 1103. The private key is preferably stored on removable media, such as a floppy disk, so that it can be stored in a secure location; though in alternative embodiments the private key may be stored in fixed media. The party clicks on Generate button 1104, and the private key is generated and stored on the specified media, according to the file name and/or path specified in field 1103 (if applicable), while the public key is sent to the Certificate Authority.

Once the keys have been generated and stored, the user may be prompted for the location of the private key (and asked to insert the removable media, if applicable) when the key is needed for authentication purposes, as described below. Additional security and/or authentication measure may also be taken, such as asking the user to re-enter the passphrase at the appropriate time.

Referring now to Figure 12, there is shown an example of a screen display 1200 for private key retrieval. In one embodiment, screen 1200 is shown whenever a

party clicks a Sign document button or otherwise indicates that he or she wishes to digitally sign a document. For authentication purposes, the party is asked to insert the floppy disk containing the previously generated private key. If appropriate, the user is asked to specify the filename and/or path for the private key in field 1201. Optionally, the user may be asked to enter a passphrase (previously selected in the example of Figure 11) in field 1202. The party then clicks on Sign button 1203 to affix the digital signature to the document.

Referring now to Figure 13, there is shown a flowchart of a document signing method according to one embodiment of the present invention. The flowchart of Figure 13 is merely illustrative of a particular method as may apply to the processing of the examples of Figures 6A-6B and 8A through 12. One skilled in the art will recognize that other variations and methods are possible and applicable to different types of documents in accordance with the present invention.

Once a document has been initiated and a party has digitally signed the document, the document is assigned 1302 a Digital Object Identifier (DOI)—a unique number or other identifier that is used to track the document. The digital signature is verified 1303 to make sure that the document is an original and that no tampering has taken place. If a digital certificate has been asserted with respect to the document, the appropriate certificate authority is contacted to determine 1304 whether the asserted certificate has been revoked. If the digital signature is reliant upon on a certificate, this step ensures that the certificate is valid and trustworthy.

The data entered by the party is checked 1305 for completeness and accuracy; such a check may include verification of a correct syntax or number combination for various fields and the like.

If, in steps 1303, 1304, or 1305 any problems are found with the signature, certificate, or completeness of data, processing may stop and the user may be alerted as to the status of the document. Otherwise, processing continues with step 1306.

Data is extracted 1306 from the completed form and provided to a back-end database (not shown). In one embodiment, the data is transmitted via Open Database Connectivity (ODBC) calls as are known in the art. The back-end database stores the extracted data for later retrieval when the document is to be reviewed or otherwise output.

Credit card, ACH, or other Electronic Funds Transfer (ECF) is issued 1307 in accordance with user-supplied account information, as collected in various fields as described above.

In some circumstances, human review of the document may be desirable before processing continues. If applicable, the document is displayed 1308 for human review.

In the example shown, a new identification number is generated 1309 for the applicant represented by the party signing the document. One skilled in the art will recognize that such a step is merely exemplary, and that any type of identification or other generated data element may be provided, as appropriate to the particular application.

A back-end server (not shown) then records 1310 that the document has been accepted and signed, and the document is stored 1311 in a database or other persistent storage. As described above, E-Cabinet 352 permits selective access to the entire document or parts thereof, in accordance with various permissions and other parameters associated with the document and/or the person seeking access. Thus, when requested by a user and in accordance with permissions, authentication requirements, and security levels, the document is retrieved from the database and displayed 1312, for example on a browser under the user's control. Referring now to Figure 14, there is shown a system block diagram of one embodiment of a document management flow process in a signing room implemented according to the present invention. One skilled in the art will recognize that the process shown in Figure 14 is merely exemplary of a particular application of the present invention in one embodiment.

A client, who may be one of the parties to a transaction, and who may be accessing the system of the present invention from a remote location, originates 1404 the signing room documents, either by generating the documents in a word processor or similar software application, or by uploading and converting existing documents. The process of creating and/or converting such documents is known in the art.

Virtual File Clerk 1405, which is a business logic tier 343 functional module which forms an interface between presentation 342 and persistent storage 344 (including database 1409), processes the originated or converted documents and manages the document flow.

As described above, presentation tier 352, implements signing room 300, E-Cabinet 352, and the like, for hosting and presenting documents, signing rooms, and the like.

Presentation tier 352 may contain any number of virtual signing rooms 300. In the example of Figure 14, three such signing rooms 300 are shown for illustrative purposes: a Proposition 209 room 300A for implementing a transaction involving government legislation; an Investment Banking Transaction room 300B for implementing an investment transaction; and a Real Estate room 300C for implementing a real estate transaction. One skilled in the art will recognize that many other types of virtual signing rooms 300 can be provided according to the present invention.

Each signing room 300 contains information describing roles 1401, content 1402, and transactions/documents 1403. For example, the Proposition 209 room 300A contains four roles 1401A (originator, moderator, participant, and observer), five content items 1402A (documents of commerce, reports, white papers, discussion threads, and multi-dimensional links), and four sets of transactions/documents 1403A (petition, supporting/opposing documents, discussions, documents to sign). The Investment Banking Transaction room 300B contains four roles 1401B (originator, moderator, participant, and observer), six content items 1402B (documents of commerce, reports, white papers, discussion threads, multi-dimensional links, and high security items), and six sets of transactions/documents 1403B (offer, supporting documents, letter of intent, evolving contract, digital signatures, and archive). The Real Estate room 300C contains four roles 1401C (originator, moderator, participant, and observer), five content items 1402C (documents of commerce, reports, white pa-

pers, discussion threads, and multi-dimensional links), and six sets of transactions/documents 1403C (listing, sale contract, loan applications, appraisals, loan documents, and deeds).

In one embodiment, an archive 1410 is provided for long-term storage of any or all elements of signing rooms 300. The archive 1410 may include, for example, a chronology of events, revision logs, drafts, and the like. The archive 1410 may be stored, for example, on a compact disc read-only memory (CD-ROM) device or the like, for convenient access at a later time.

Referring now to Figure 15, there is shown a system block diagram of one embodiment of a document management flow process in a disclosure room implemented according to the present invention. One skilled in the art will recognize that the process shown in Figure 15 is merely exemplary of a particular application of the present invention in one embodiment.

In several respects, the disclosure room process of Figure 15 is similar to the signing room process previously described in connection with Figure 14, although in general, in a disclosure room, no application of digital signatures takes place. The client originates 1404 the disclosure room documents, either by generating the documents in a word processor or similar software application, or by uploading and converting existing documents. As before, the process of creating and/or converting such documents is known in the art. Virtual File Clerk 1405 processes the originated or converted documents and manages the document flow. Presentation tier 342 implements signing room 300, E-Cabinet 352, and the like, for hosting and presenting

documents, interfacing with database 1502. In addition, traffic relating to the disclosure room can be archived 1507, if desired.

Presentation tier 342 may contain any number of virtual disclosure rooms 1503. In the example of Figure 15, one such signing room 1503 is shown for illustrative purposes: a Technology Preview room 1503. One skilled in the art will recognize that many other types of virtual disclosure rooms 1503 can be provided according to the present invention.

Each disclosure room 1503 contains information describing roles 1504, content 1505, and transactions/documents 1506. For example, the Technology Preview room 1503 contains four roles 1504 (originator, moderator, participant, and observer), six content items 1505 (documents of commerce, reports, white papers, discussion threads, multi-dimensional links, and high security items), and five sets of transactions/documents 1506 (confidential specifications, documentation, disclosure agreement, digital signatures, and archives).

As with the example of Figure 14, in one embodiment, an archive 1410 is provided for long-term storage of any or all elements of signing room 1503. The archive 1410 may include, for example, a chronology of events, revision logs, drafts, and the like. The archive 1410 may be stored, for example, on a compact disc read-only memory (CD-ROM) device or the like, for convenient access at a later time.

Referring now to Figure 16A, there is shown a flowchart showing a signing room logon and entry method according to one embodiment of the present invention. In one embodiment, the steps of Figure 16A are performed by presentation tier 342 as described above in the context of the overall architecture. A user logs on 2301

to the signing room to obtain access to documents and other materials. As described above, the user access the system of the present invention over a network such as the Internet, using, for example, a browser. The user is presented with a contract describing terms of use of the virtual signing room, which he or she reads 2302. If the user deems the terms to be satisfactory, he or she indicates agreement 2303 to the terms, for example by clicking on an onscreen button.

Once the user has indicated agreement, he or she arranges for payment 2304 for the virtual signing room service, such as for example by supplying a credit card number or enabling electronic funds transfer. The system of the present invention collects payment in accordance with the user's specifications, using techniques that are known in the art.

The user then selects 2305 a security level for the virtual signing room. In one embodiment, the user can select from five security levels, though one skilled in the art will recognize that any number of security levels may be provided. In one embodiment, each of the security levels is associated with a different level and/or type of party authentication, including for example verification by passphrase, biometric data, smartcard, IP address, processor ID code, and the like.

The user then selects 2306 a signing room to enter. This step may entail various substeps as described in more detail in connection with Figure 16B. The user is then given an opportunity to calendar 2307 discussion, editing, and signing events within the context of the virtual signing room. Thus, various transaction-related events and items can be scheduled, depending on the nature and structure of the particular deal. In one embodiment, the calendared events are stored so that an

overall schedule of the events can be retrieved, modified, or otherwise accessed when needed.

The user enters 2308 a signing room, for example by selecting from a displayed list of available rooms to which the user has access. The user may select one of the displayed rooms, for example by clicking on an onscreen button or link. The user then verifies his or her identity, providing the appropriate input in accordance with the signing room's security level, and further verifies the role to which the user has been assigned. The present invention then allows the user to actively participate in the signing room activities, including viewing, modification, and signing of documents as his or her access level permits.

If desired, and if the access level permits such an operation, the user may create 2309 a new document within the virtual signing room. In one embodiment, the user creates a new document by selecting from a number of available document templates, filling in additional information as appropriate for the selected template, attaching a digital signature (if applicable), and submitting the document to the virtual signing room. The document may then be made available to other users in the room, if appropriate.

Referring to Figure 16B, there is shown a flowchart depicting a signing room admittance procedure according to one embodiment of the present invention. In one embodiment, the steps of Figure 16B are performed by presentation tier 342 as described above in the context of the overall architecture. The method of Figure 16B may be performed, for example, in the context of selecting a signing room as in step 2306 of Figure 16A.

When a user selects a signing room for access, the present invention verifies 2401 the permissions associated with the signing room, to ensure that the user is in fact permitted to access the specified room. The user selects 2402 a role, as described above, for his or her interaction with the documents and other parties in the signing room. Other participants in the room are then notified 2403 of the presence of the user, either by display of a dialog box, or an icon or other indicator, or by some other means. If appropriate, the user is also added 2404 to any discussion groups that may be taking place in the context of the room.

The user is also given an opportunity to check in documents that he or she may have been creating and/or modified in an off-line environment. The user sets up 2405 permissions for the documents being checked in, and defines 2406 any required processes associated with the documents (such as a signing sequence or other transaction-related steps). The user also identifies 2407 the location or DOI of the documents being checked in. A test may be performed 2408 of the virtual form of the document (in other words, the representation of the document within the context of the virtual signing room).

In addition, the user may define 2409 the outputs for the signing room, including for example whether templates, document creation or editing, and/or transactional signatures are to be provided in the context of the signing room.

Referring now to Figure 16C, there is shown a flowchart depicting an account termination method according to one embodiment of the present invention. The method of Figure 16C may be performed, for example, when a user wishes to terminate a signing room, such as when a transaction is completed or aborted. Upon re-

ceipt of a user's request to terminate a signing room, the user's identity is verified 2501, as are the user's rights in connection with account termination. If the identity rights are verified appropriately, the signing room is archived 2502 (such as to a CD-ROM), and the signing room is deleted 2503.

In one embodiment, participants in the room are warned of the impending deletion of the room. In alternative embodiments, the assent of other participants is sought prior to deletion. Each party may then request a copy of the archive (CD-ROM), if desired and appropriate.

Referring now to Figure 17, there is shown a flowchart depicting an example of an electronic signature collection method according to one embodiment of the present invention. The method of Figure 17 illustrates a particular application of the present invention to the electronic collection of signatures for a petition. As such, the various elements and specific components of Figure 17 are merely exemplary.

The invention presents a welcome screen 1701, as may be provided using a web page viewable in a browser application. The welcome screen 1701 includes a link or button allowing the user to access a selected initiative for viewing and/or signing. Once the user has selected an initiative, he or she selects 1702 a county from a displayed list. In some cases, the displayed petition will vary depending on the selected county.

The user is then presented with an entry screen 1703 for the virtual signing room. The user is asked to select one of four roles, depending on the activity he or she would like to perform with respect to the signing room. In the example of Fig-

ure 17, the four available roles are petition viewer, petition signer, circulator (whose function is to witness signatures and answer questions), and administrator.

If in screen 1703 the user selects the petition viewer role, the invention displays a view petition screen 1704 from which the user can select various items for viewing. In the context of a petition, examples include a proponent's statement, an opponent's statement, press releases, and the like. In addition, a chat room facilitating real-time communication may be provided and accessible from screen 1704, using techniques that are known in the art.

If in screen 1703 the user selects the petition signer role, the invention determines 1705 whether the user has previously set up a digital signature, as described above. If so, the signature is verified 1706, and the user is given an opportunity to sign 1708 the petition. In the context of a petition signing application, certain items of information may be presented and/or collected in the course of the signing operation of step 1708, as shown in Figure 17. In one embodiment, drop-down lists may be provided in the sign petition screen 1708, allowing the signer to "place" identifying information within the petition document itself in the course of signing it.

If in step 1705 the invention determines that the user has not previously set up a digital signature, the user is prompted to enter identifying information (such as driver's license number, social security number, and the like) to initiate the process of configuring a new digital signature. Once the digital signature has been enabled, the invention proceeds with step 1708.

After step 1708 has been completed, the invention determines 1709 whether the registration data supplied by the user is valid. If so, the petition is signed 1710.

Registration is reported as complete, the user is prompted to click a button to apply the signature, a key pair is generated, the petition is signed with the private key, the private key is deleted, a public key is attached to the petition, and the petition is stored. If in step 1709 the registration data is not valid, the petition is not signed 1711. Registration is reported as not complete, a chat is initiated with the circulator to resolve the registration problem, new registration data is obtained, and data is submitted for matching with a registered voter list. Step 1709 may then be re-attempted with the new registration data.

If in screen 1703 the user selects the circulator role, a logon/logoff screen 1712 is presented allowing the user to specify whether he or she wishes to log on or log off. If logon is selected, the user is presented with a logon screen 1713. If logoff is selected, he or she is presented with a logoff screen 1714. Once the circulator has logged on, he or she is able to perform relevant activities as are applicable, such as witness signatures and the like.

If in screen 1703 the user selects the administrator role, several administrator functions become available 1715, such as:

- setting up a new initiative;
- creating a new circulator;
- generating reports on signatures;
- generating totals;
- generating county subtotals;
- generating disk-based signature lists;

- generating holographic labels for circulator use (where states may require that the circulator prepare a label in his or her own handwriting);
- generating tools for county election officials to tabulate, verify, and/or withdraw signatures.

As mentioned previously, the specific items listed above in connection with the example of Figure 17 are merely exemplary of one embodiment of the present invention.

Referring now to Figures 18A-D, there are shown screen shots depicting an example of a signing room according to one embodiment of the present invention. Home page 1800 provides the user with options for selecting roles such as petition viewer, petition signer, circulator, and administrator, as described above in step 1703 of Figure 17. Signing room 1801 shows an example of a petition as displayed in accordance with the petition signer role. The title and a summary of the petition are displayed, and the user is given an opportunity to digitally sign the petition as described in step 1708 of Figure 17. In the example of Figure 18B, the user is prompted for a first name, middle name or initial, last name, address, city, ZIP code, and either a social security number or California driver's license number, in order to initialize the digital signature.

Page 1802, which may be displayed in connection with step 1710 of Figure 17, confirms to the user that he or she is registered and may sign the petition by clicking on the appropriate on-screen button 1804.

Page 1803, which may be displayed in connection with step 1711 of Figure 17, opens a chat session with the circulator in order to resolve registration issues. The

user can then communicate with the circulator over the chat channel, in accordance with known techniques for on-line instant messaging or "chat".

Referring now to Figure 19, there is shown a flowchart depicting a deed recording method according to one embodiment of the present invention. The particular sequence of steps shown in Figure 19 may be performed, for example, by a computer or set of computers following a set of instructions specified in software code. The sample method of Figure 19 illustrates an application of the present invention to a simple deed recording transaction, though one skilled in the art will recognize that other types of transactions, including more complex transactions, could be enabled using the present invention. A user prepares 1901 the deed using a conventional browser interface with form fields and the like. Upon completion, the deed is automatically e-mailed 1902 to a recorder and received 1903 at a central server (not shown). The invention parses 1904 the received deed in order to extract information for storage in the database 1409; in addition, if the deed has been digitally signed, information describing or confirming the digital signature is stored. If in 1905 a filing fee is to be collected, the fee is collected 1906, for example by charging the user's credit card or by effecting an electronic funds transfer.

If in 1907 the deed is not recordable, it is returned 1908 to the originator with an explanation of the rejection. If it is recordable, the invention verifies 1909 the document integrity 1909 and the digital signature 1910. If in 1911 the document is not approved (e.g. due to problems with document integrity and/or signatures), it is returned 1912 to the originator with an explanation of the rejection.

If the document is approved, the deed is recorded 1913 and a notice of recording is returned 1914. The deed, in digital form, is stored 1915 in database 1409 for future use and access. Database 1409 is updated 1916 to reflect the recorded deed. In addition, if desired, the deed is transmitted 1917 to the assessor, printed 1918 to paper, and/or printed 1919 to microfiche.

The above description is included to illustrate the operation of the preferred embodiments and is not meant to limit the scope of the invention. The scope of the invention is to be limited only by the following claims. From the above discussion, many variations will be apparent to one skilled in the art that would yet be encompassed by the spirit and scope of the present invention.

Appendix A

The following is an example of an XML-encoded document 102 corresponding to the agreement document depicted in Figures 6A-6B. One skilled in the art will recognize that the document may be encoded by other means and in other languages adapted to numerous specific applications and contexts.

```
- <XML>
  - <BODY background="sandstrip_bkg_frame.gif">
    - <TABLE width="500">
      - <TR>
        - <TD>
            <IMG alt="" src="logo_midsize.gif" />
          </TD>
        - <TD align="right">
            powered by
            <BR />
            <IMG alt="" src="Hi Res Logo5trans.gif"
              style="HEIGHT: 31px; WIDTH: 137px" />
            <BR />
            Patents Pending
            <BR />
          </TD>
        </TR>
      </TABLE>
    - <FONT face="Tahoma">
        <STRONG>U.S. Distributor Application & Agreement</STRONG>
      </FONT>
      <P />
    - <TBS id="Morinda">
      - <TBS id="Applicant">
        - <TABLE>
          - <TR>
            - <TD align="right">
                <STRONG>Personal Information</STRONG>
              </TD>
            - <TD>
                (
                <FONT color="red">*</FONT>
                Required Information)
              </TD>
            </TR>
          - <TR>
              <TD align="right">Applicant's Name</TD>
            - <TD>
              - <AppName>
                  <INPUT value="*Last, First, Middle"
                    size="30" style="BACKGROUND-COLOR:
                    bisque" />
                </AppName>
              </TD>
            </TR>
          - <TR>
              <TD align="right">Applicant's SS Number</TD>
            - <TD>
```

```
      - <AppSSN>
          <INPUT size="11" style="BACKGROUND-
            COLOR: bisque" value="*nnn-nn-nnnn" />
        </AppSSN>
        <INPUT type="button" value="Note"
          style="BACKGROUND-COLOR: tan" on-
          Click="alert('The Social Security Number
          is absolutely required.')" />
      </TD>
    </TR>
  - <TR>
      <TD align="right">Spouse (or Co-Applicant's
        Name)</TD>
    - <TD>
      - <CoAppName>
          <INPUT size="30" style="BACKGROUND-
            COLOR: bisque" value="Last, First,
            Middle" />
        </CoAppName>
        <INPUT type="button" value="Note"
          style="BACKGROUND-COLOR: tan" on-
          Click="alert('Having a co-applicant is op-
          tional. It is highly recommended that the
          spouse information be filled out as the
          spouse is considered as having a benefi-
          cial interest in the distributorship.')"
          />
      </TD>
    </TR>
  - <TR>
      <TD align="right">Spouse (or Co-Applicant's)
        SSN</TD>
    - <TD>
      - <CoAppSSN>
          <INPUT size="11" style="BACKGROUND-
            COLOR: bisque" value="nnn-nn-nnnn" />
        </CoAppSSN>
      </TD>
    </TR>
  - <TR>
      <TD align="right">U.S. Mailing Address</TD>
    - <TD>
      - <AppAdd>
          <INPUT size="30" value="*"
            style="BACKGROUND-COLOR: bisque" />
        </AppAdd>
        <INPUT type="button" value="Note"
          style="BACKGROUND-COLOR: tan" on-
          Click="alert('We must have a second ad-
          dress for shipping if your mailing address
          is a PO Box, or if you would like your
          AutoShip sent to an alternate address.')"
          />
      </TD>
    </TR>
  - <TR>
      <TD align="right">City, State, Zip Code</TD>
    - <TD>
      - <AppCity>
          <INPUT size="10" value="*"
            style="BACKGROUND-COLOR: bisque" />
        </AppCity>
      - <AppST>
        - <SELECT size="1" style="BACKGROUND-
            COLOR: bisque">
            <OPTION>AL</OPTION>
```

```
                <OPTION>AK</OPTION>
                <OPTION>AZ</OPTION>
                <OPTION>AR</OPTION>
                <OPTION SELECTED="">CA</OPTION>
                <OPTION>CO</OPTION>
                <OPTION>CN</OPTION>
                <OPTION>DE</OPTION>
                <OPTION>FL</OPTION>
                <OPTION>GA</OPTION>
                <OPTION>HA</OPTION>
                <OPTION>ID</OPTION>
                <OPTION>IL</OPTION>
                <OPTION>IN</OPTION>
                <OPTION>IO</OPTION>
                <OPTION>KA</OPTION>
                <OPTION>KY</OPTION>
                <OPTION>LO</OPTION>
                <OPTION>ME</OPTION>
                <OPTION>MD</OPTION>
                <OPTION>MA</OPTION>
                <OPTION>MI</OPTION>
                <OPTION>MN</OPTION>
                <OPTION>MO</OPTION>
                <OPTION>MT</OPTION>
                <OPTION>NE</OPTION>
                <OPTION>NV</OPTION>
                <OPTION>NH</OPTION>
                <OPTION>NJ</OPTION>
                <OPTION>NM</OPTION>
                <OPTION>NY</OPTION>
                <OPTION>NC</OPTION>
                <OPTION>ND</OPTION>
                <OPTION>OH</OPTION>
                <OPTION>OK</OPTION>
                <OPTION>OR</OPTION>
                <OPTION>PN</OPTION>
                <OPTION>RI</OPTION>
                <OPTION>SC</OPTION>
                <OPTION>SD</OPTION>
                <OPTION>TN</OPTION>
                <OPTION>TX</OPTION>
                <OPTION>UT</OPTION>
                <OPTION>VT</OPTION>
                <OPTION>VI</OPTION>
                <OPTION>WA</OPTION>
                <OPTION>WV</OPTION>
                <OPTION>WI</OPTION>
                <OPTION>WY</OPTION>
              </SELECT>
            </AppST>
          - <AppZip>
              <INPUT style="BACKGROUND-COLOR: bisque"
                size="8" value="*nnnnn-nnnn" />
            </AppZip>
          </TD>
        </TR>
      - <TR>
          <TD align="right">Date of Birth</TD>
        - <TD>
          - <AppDOB>
            - <SELECT size="1" style="BACKGROUND-
                COLOR: bisque">
                <OPTION selected="">Jan</OPTION>
                <OPTION>Feb</OPTION>
                <OPTION>Mar</OPTION>
                <OPTION>Apr</OPTION>
```

```
      <OPTION>May</OPTION>
      <OPTION>Jun</OPTION>
      <OPTION>Jul</OPTION>
      <OPTION>Aug</OPTION>
      <OPTION>Sep</OPTION>
      <OPTION>Oct</OPTION>
      <OPTION>Nov</OPTION>
      <OPTION>Dec</OPTION>
    </SELECT>
  - <SELECT size="1" style="BACKGROUND-
      COLOR: bisque">
      <OPTION selected="">01</OPTION>
      <OPTION>02</OPTION>
      <OPTION>03</OPTION>
      <OPTION>04</OPTION>
      <OPTION>05</OPTION>
      <OPTION>06</OPTION>
      <OPTION>07</OPTION>
      <OPTION>08</OPTION>
      <OPTION>09</OPTION>
      <OPTION>10</OPTION>
      <OPTION>11</OPTION>
      <OPTION>12</OPTION>
      <OPTION>13</OPTION>
      <OPTION>14</OPTION>
      <OPTION>15</OPTION>
      <OPTION>16</OPTION>
      <OPTION>17</OPTION>
      <OPTION>18</OPTION>
      <OPTION>19</OPTION>
      <OPTION>20</OPTION>
      <OPTION>21</OPTION>
      <OPTION>22</OPTION>
      <OPTION>23</OPTION>
      <OPTION>24</OPTION>
      <OPTION>25</OPTION>
      <OPTION>26</OPTION>
      <OPTION>27</OPTION>
      <OPTION>28</OPTION>
      <OPTION>29</OPTION>
      <OPTION>30</OPTION>
      <OPTION>31</OPTION>
    </SELECT>
    ,19
  - <SELECT size="1" style="BACKGROUND-
      COLOR: bisque">
      <OPTION selected="">0</OPTION>
      <option>1</option>
      <option>2</option>
      <option>3</option>
      <option>4</option>
      <option>5</option>
      <option>6</option>
      <option>7</option>
      <option>8</option>
      <option>9</option>
    </SELECT>
  - <SELECT size="1" style="BACKGROUND-
      COLOR: bisque">
      <option selected="">0</option>
      <option>1</option>
      <option>2</option>
      <option>3</option>
      <option>4</option>
      <option>5</option>
      <option>6</option>
```

```
            <option>7</option>
            <option>8</option>
            <option>9</option>
          </SELECT>
        </AppDOB>
        <INPUT type="button" value="Note"
          style="BACKGROUND-COLOR: tan" on-
          Click="alert('This is needed as verifica-
          tion that the new distributor is of legal
          age to be a distributor in the state of
          their residency.')" />
      </TD>
    </TR>
  - <TR>
      <TD align="right">Daytime Phone</TD>
    - <TD>
      - <AppDPh>
          <INPUT size="10" style="BACKGROUND-
            COLOR: bisque" value="*nnn-nnn-nnnn"
            />
        </AppDPh>
        <INPUT type="button" value="Note"
          style="BACKGROUND-COLOR: tan" on-
          Click="alert('Please indicate the numbers
          where you may be reached.')" />
      </TD>
    </TR>
  - <TR>
      <TD align="right">Alternate Phone</TD>
    - <TD>
      - <AppOPh>
          <INPUT size="10" style="BACKGROUND-
            COLOR: bisque" value="*nnn-nnn-nnnn"
            />
        </AppOPh>
      </TD>
    </TR>
  - <TR>
      <TD align="right">Evening Phone</TD>
    - <TD>
      - <AppEPh>
          <INPUT size="10" style="BACKGROUND-
            COLOR: bisque" value="*nnn-nnn-nnnn"
            />
        </AppEPh>
      </TD>
    </TR>
  - <TR>
      <TD align="right">Cellular Phone</TD>
    - <TD>
      - <AppCPh>
          <INPUT size="10" style="BACKGROUND-
            COLOR: bisque" value="nnn-nnn-nnnn" />
        </AppCPh>
      </TD>
    </TR>
  - <TR>
      <TD align="right">FAX</TD>
    - <TD>
      - <AppFAX>
          <INPUT size="10" style="BACKGROUND-
            COLOR: bisque" value="nnn-nnn-nnnn" />
        </AppFAX>
      </TD>
    </TR>
  - <TR>
```

```
      <TD align="right">E-Mail Address</TD>
    - <TD>
      - <AppEM>
          <INPUT style="BACKGROUND-COLOR: bisque"
            size="30" />
        </AppEM>
      </TD>
    </TR>
  - <TR>
      <TD align="right" />
    - <TD>
        <INPUT type="button" value="Generate Keys"
          onclick="navigate('morindagenerate.htm')"
          style="BACKGROUND-COLOR: tan" />
        <INPUT type="button" value="Explain" on-
          click="navigate('http://www.whatis.com/pki
          .htm')" style="BACKGROUND-COLOR: tan" />
      </TD>
    </TR>
  - <TR>
      <TD align="right" />
      <TD />
    </TR>
  - <TR>
    - <TD align="right">
        <STRONG>*Personal Sponsor's Informa-
          tion</STRONG>
      </TD>
    - <TD>
        The distributor that referred you to the
        company.
        <BR />
        Placement and personal sponsors may be the
        same.
        <INPUT style="BACKGROUND-COLOR: tan" on-
          click="alert('Your placement and personal
          sponsor may be the same distributor if you
          are on the personal sponsors first level
          and have not been placed.')" type="button"
          value="Note" />
      </TD>
    </TR>
  - <TR>
      <TD align="right">Name</TD>
    - <TD>
      - <PSIName>
          <INPUT size="30" style="BACKGROUND-
            COLOR: bisque" value="*Last, First,
            Middle" />
        </PSIName>
      </TD>
    </TR>
  - <TR>
      <TD align="right">Phone</TD>
    - <TD>
      - <PSIPh>
          <INPUT size="10" style="BACKGROUND-
            COLOR: bisque" value="nnn-nnn-nnnn" />
        </PSIPh>
      </TD>
    </TR>
  - <TR>
      <TD align="right">ID Number</TD>
    - <TD>
      - <PSINum>
```

```
            <INPUT size="8" style="BACKGROUND-COLOR:
              bisque" value="nnnnnnnn" />
          </PSINum>
        </TD>
      </TR>
    - <TR>
        <TD align="right" />
        <TD />
      </TR>
    - <TR>
      - <TD align="right">
          <STRONG>Placement Information</STRONG>
        </TD>
      - <TD>
          It is highly recommended that you
        - <STRONG>
            <EM>NOT</EM>
          </STRONG>
          fill out placement information upon sign-up.
          <INPUT onclick="alert('The Placement Sponsor
            is the distributor that you are placed di-
            rectly under. Placement sponsor must be in
            the downline of your Personal sponsor. It
            is highly recommended that you NOT fill
            out placement information upon sign-up.
            Leaving it blank will give your personal
            sponsor 120 days to determine where to
            place you using a placement sponsor change
            form. This is your one placement. If you
            are placed anywhere other than your Per-
            sonal Sponsors first level, you cannot be
            moved.')" style="BACKGROUND-COLOR: tan"
            type="button" value="Note" />
        </TD>
      </TR>
    - <TR>
        <TD align="right">Name</TD>
      - <TD>
        - <PIName>
            <INPUT size="30" style="BACKGROUND-
              COLOR: bisque" value="Last, First,
              Middle" />
          </PIName>
        </TD>
      </TR>
    - <TR>
        <TD align="right">Phone</TD>
      - <TD>
        - <PIPh>
            <INPUT size="10" style="BACKGROUND-
              COLOR: bisque" value="nnn-nnn-nnnn" />
          </PIPh>
        </TD>
      </TR>
    - <TR>
        <TD align="right">ID Number</TD>
      - <TD>
        - <PINum>
            <INPUT size="8" style="BACKGROUND-COLOR:
              bisque" value="nnnnnnnn" />
          </PINum>
        </TD>
      </TR>
    - <TR>
        <TD align="right" />
        <TD />
```

```
    </TR>
  - <TR>
    - <TD align="right">
        <STRONG>Case AutoShip Program</STRONG>
      </TD>
    - <TD>
        <INPUT type="button" value="Enroll" on-
          click="navigate('morindaauto.htm')"
          style="BACKGROUND-COLOR: tan" />
        me in Morinda's Case AutoShip Program.
      </TD>
    </TR>
  - <TR>
      <TD align="right" />
      <TD />
    </TR>
  - <TR>
    - <TD align="right">
        <STRONG>Nonresident Alien Distribu-
          tors</STRONG>
      </TD>
    - <TD>
      - <AppAlien>
          <INPUT type="checkbox"
            style="BACKGROUND-COLOR: bisque" />
        </AppAlien>
        I am living in the United States, but am not
        a U.S. Citizen. Nonresident Aliens in the
        U.S. are required by law to submit an IRS
        Form W-8
      </TD>
    </TR>
  - <TR>
      <TD align="right" />
      <TD />
    </TR>
  - <TR>
    - <TD align="right">
        <STRONG>Sign-up fee</STRONG>
      </TD>
      <TD>non-refundable $20.00</TD>
    </TR>
  - <TR>
      <TD align="right">Method of payment</TD>
    - <TD>
      - <AppPay>
        - <SELECT size="1" style="BACKGROUND-
            COLOR: bisque">
            <OPTION selected="">VISA</OPTION>
            <OPTION>M/C</OPTION>
            <OPTION>DISCOVER</OPTION>
          </SELECT>
        </AppPay>
        OR
        <INPUT type="button" value="ACH" on-
          click="navigate('morindaACH.htm')"
          style="BACKGROUND-COLOR: tan" />
      </TD>
    </TR>
  - <TR>
      <TD align="right">Credit Card #</TD>
    - <TD>
      - <AppCCN>
          <INPUT style="BACKGROUND-COLOR: bisque"
            />
        </AppCCN>
```

```
            Exp Date
          - <AppED>
            - <SELECT size="1" style="BACKGROUND-
                COLOR: bisque">
                <OPTION selected="">Jan</OPTION>
                <OPTION>Feb</OPTION>
                <OPTION>Mar</OPTION>
                <OPTION>Apr</OPTION>
                <OPTION>May</OPTION>
                <OPTION>Jun</OPTION>
                <OPTION>Jul</OPTION>
                <OPTION>Aug</OPTION>
                <OPTION>Sep</OPTION>
                <OPTION>Oct</OPTION>
                <OPTION>Nov</OPTION>
                <OPTION>Dec</OPTION>
              </SELECT>
            - <SELECT size="1" style="BACKGROUND-
                COLOR: bisque">
                <OPTION selected="">1999</OPTION>
                <OPTION>2000</OPTION>
                <OPTION>2001</OPTION>
                <OPTION>2002</OPTION>
                <OPTION>2003</OPTION>
                <OPTION>2004</OPTION>
              </SELECT>
            </AppED>
          </TD>
        </TR>
      - <TR>
          <TD align="right" />
          <TD />
        </TR>
      - <TR>
        - <TD align="right" valign="top">
            <STRONG>Signature</STRONG>
          </TD>
          <TD>The undersigned hereby applies to become an
            independent distributor of Morinda, Inc. As an
            independent distributor, I agree to the Terms
            and Conditions and in the Morinda Distributor
            Manual.</TD>
        </TR>
      - <TR>
        - <TD colspan="2" align="middle">
            <TEXTAREA readOnly="" style="BACKGROUND-
              COLOR: bisque; HEIGHT: 122px; WIDTH:
              500px">TERMS AND AGREEMENT: Distributor
              and Morinda Inc. (Morinda) hereby agree to
              the following terms and conditions:
              ......</TEXTAREA>
          </TD>
        </TR>
      - <TR>
          <TD align="right" />
        - <TD>
            <INPUT type="button" value="Sign Document"
              style="BACKGROUND-COLOR: tan" on-
              click="navigate('morindasign1.htm')" />
          </TD>
        </TR>
      </TABLE>
    </TBS>
    <SIGN id="Applicant" />
  </TBS>
  <SIGN id="Morinda" />
```

```
    <CERT id="Applicant" />
    <CERT id="Morinda" />
  </BODY>
</XML>
```

Appendix B

The following is an example of an XML-encoded document 102 corresponding to the agreement document depicted in Figures 6A-6B, after it has been completed and digitally signed. One skilled in the art will recognize that the document may be encoded by other means and in other languages adapted to numerous specific applications and contexts.

```
- <XML>
  - <BODY background="sandstrip_bkg_frame.gif">
    - <TABLE width="500">
      - <TR>
        - <TD>
            <IMG alt="" src="logo_midsize.gif" />
          </TD>
        - <TD align="right">
            powered by
            <BR />
            <IMG alt="" src="Hi Res Logo5trans.gif"
              style="HEIGHT: 31px; WIDTH: 137px" />
            <BR />
            Patents Pending
            <BR />
          </TD>
        </TR>
      </TABLE>
    - <FONT face="Tahoma">
        <STRONG>U.S. Distributor Application & Agreement</STRONG>
      </FONT>
      <P />
    - <TBS id="Morinda">
      - <TBS id="Applicant">
        - <TABLE>
          - <TR>
            - <TD align="right">
                <STRONG>Personal Information</STRONG>
              </TD>
            - <TD>
                (
                <FONT color="red">*</FONT>
                Required Information)
              </TD>
            </TR>
          - <TR>
              <TD align="right">Applicant's Name</TD>
            - <TD>
                <AppName>BROWN, BRUCE</AppName>
              </TD>
            </TR>
          - <TR>
              <TD align="right">Applicant's SS Number</TD>
            - <TD>
```

```
      <AppSSN>529-66-2094</AppSSN>
    </TD>
  </TR>
- <TR>
    <TD align="right">Spouse (or Co-Applicant's
      Name)</TD>
  - <TD>
      <CoAppName>BROWN, PATTI</CoAppName>
    </TD>
  </TR>
- <TR>
    <TD align="right">Spouse (or Co-Applicant's)
      SSN</TD>
  - <TD>
      <CoAppSSN>528-76-2759</CoAppSSN>
    </TD>
  </TR>
- <TR>
    <TD align="right">U.S. Mailing Address</TD>
  - <TD>
      <AppAdd>1684 North Sage Hen Road</AppAdd>
    </TD>
  </TR>
- <TR>
    <TD align="right">City, State, Zip Code</TD>
  - <TD>
      <AppCity>OREM</AppCity>
      <AppST>UT</AppST>
      <AppZip>84097-2317</AppZip>
    </TD>
  </TR>
- <TR>
    <TD align="right">Date of Birth</TD>
  - <TD>
      <AppDOB>FEB 01, 1952</AppDOB>
    </TD>
  </TR>
- <TR>
    <TD align="right">Daytime Phone</TD>
  - <TD>
      <AppDPh>801-852-8800</AppDPh>
    </TD>
  </TR>
- <TR>
    <TD align="right">Alternate Phone</TD>
  - <TD>
      <AppOPh />
    </TD>
  </TR>
- <TR>
    <TD align="right">Evening Phone</TD>
  - <TD>
      <AppEPh>801-225-0983</AppEPh>
    </TD>
  </TR>
- <TR>
    <TD align="right">Cellular Phone</TD>
  - <TD>
      <AppCPh>801-376-0983</AppCPh>
    </TD>
  </TR>
- <TR>
    <TD align="right">FAX</TD>
  - <TD>
      <AppFAX>801-852-8810</AppFAX>
    </TD>
```

```
  </TR>
- <TR>
    <TD align="right">E-Mail Address</TD>
  - <TD>
      <AppEM>bruce@ilumin.com</AppEM>
    </TD>
  </TR>
- <TR>
    <TD align="right" />
    <TD />
  </TR>
- <TR>
  - <TD align="right">
      <STRONG>*Personal Sponsor's Informa-
        tion</STRONG>
    </TD>
  - <TD>
      The distributor that referred you to the
      company.
      <BR />
      Placement and personal sponsors may be the
      same.
      <INPUT style="BACKGROUND-COLOR: tan" on-
        click="alert('Your placement and personal
        sponsor may be the same distributor if you
        are on the personal sponsors first level
        and have not been placed.')" type="button"
        value="Note" />
    </TD>
  </TR>
- <TR>
    <TD align="right">Name</TD>
  - <TD>
      <PSIName>ISRAELSEN, D. BRENT</PSIName>
    </TD>
  </TR>
- <TR>
    <TD align="right">Phone</TD>
  - <TD>
      <PSIPh>801-376-6166</PSIPh>
    </TD>
  </TR>
- <TR>
    <TD align="right">ID Number</TD>
  - <TD>
      <PSINum>11223344</PSINum>
    </TD>
  </TR>
- <TR>
    <TD align="right" />
    <TD />
  </TR>
- <TR>
  - <TD align="right">
      <STRONG>Placement Information</STRONG>
    </TD>
  - <TD>
      It is highly recommended that you
    - <STRONG>
        <EM>NOT</EM>
      </STRONG>
      fill out placement information upon sign-up.
      <INPUT onclick="alert('The Placement Sponsor
        is the distributor that you are placed di-
        rectly under. Placement sponsor must be in
        the downline of your Personal sponsor. It
```

```
            is highly recommended that you NOT fill
            out placement information upon sign-up.
            Leaving it blank will give your personal
            sponsor 120 days to determine where to
            place you using a placement sponsor change
            form. This is your one placement. If you
            are placed anywhere other than your Per-
            sonal Sponsors first level, you cannot be
            moved.')" style="BACKGROUND-COLOR: tan"
            type="button" value="Note" />
        </TD>
      </TR>
    - <TR>
        <TD align="right">Name</TD>
      - <TD>
          <PIName />
        </TD>
      </TR>
    - <TR>
        <TD align="right">Phone</TD>
      - <TD>
          <PIPh />
        </TD>
      </TR>
    - <TR>
        <TD align="right">ID Number</TD>
      - <TD>
          <PINum />
        </TD>
      </TR>
    - <TR>
        <TD align="right" />
        <TD />
      </TR>
    - <TR>
        <TD align="right" />
        <TD />
      </TR>
    - <TR>
      - <TD align="right">
          <STRONG>Nonresident Alien Distribu-
            tors</STRONG>
        </TD>
      - <TD>
          <AppAlien>no</AppAlien>
          I am living in the United States, but am not
          a U.S. Citizen. Nonresident Aliens in the
          U.S. are required by law to submit an IRS
          Form W-8
        </TD>
      </TR>
    - <TR>
        <TD align="right" />
        <TD />
      </TR>
    - <TR>
      - <TD align="right">
          <STRONG>Sign-up fee</STRONG>
        </TD>
        <TD>non-refundable $20.00</TD>
      </TR>
    - <TR>
        <TD align="right">Method of payment</TD>
      - <TD>
          <AppPay>VISA</AppPay>
        </TD>
```

```
        </TR>
      - <TR>
          <TD align="right">Credit Card #</TD>
        - <TD>
            <AppCCN>3752-xxxxx-xxxx</AppCCN>
            Exp Date
            <AppED>Jan 2002</AppED>
          </TD>
        </TR>
      - <TR>
          <TD align="right" />
          <TD />
        </TR>
      - <TR>
        - <TD align="right" valign="top">
            <STRONG>Signature</STRONG>
          </TD>
          <TD>The undersigned hereby applies to become an
            independent distributor of Morinda, Inc. As an
            independent distributor, I agree to the Terms
            and Conditions and in the Morinda Distributor
            Manual.</TD>
        </TR>
      - <TR>
        - <TD colspan="2" align="middle">
            <TEXTAREA readOnly="" style="BACKGROUND-
              COLOR: bisque; HEIGHT: 122px; WIDTH:
              500px">TERMS AND AGREEMENT: Distributor
              and Morinda Inc. (Morinda) hereby agree to
              the following terms and conditions:
              ......</TEXTAREA>
          </TD>
        </TR>
      - <TR>
          <TD align="right" />
          <TD />
        </TR>
      </TABLE>
    </TBS>
    Digital Signature of Applicant
    <BR />
    <SIGN id="Applicant">1a 11 7c 4b c9 00 c3 dc 54 6e 3d c7 1b c4
      6a 30 b7 54 5a 1c 71 48 c8 ec be f8 dd fd ce f0 17 3d 17 05
      d7 cd fb 47 37 d3 9c de ff 3b 64 0b 1a 4c 15 5b 7e cb a3 c4
      bb 1e 84 37 2b 20 60 9c 83 0c</SIGN>
    <BR />
  </TBS>
  <SIGN id="Morinda" />
  Certificate of Applicant
  <BR />
  <CERT id="Applicant">e9 be 75 71 74 30 f2 96 8f 73 47 ee 43 c9 71
    ec 27 98 6d 16 5b ec 55 e4 e5 81 9c c2 30 52 1a f9 31 b3 55 06
    02 dc 15 d1 02 11 41 b6 bc 5a 9f d8 54 97 3a 02 8d 7c ca 2a 2c
    7c f1 9a 8c 79 fe 54</CERT>
  <CERT id="Morinda" />
 </BODY>
</XML>
```

Claims

What is claimed is:

1. A computer-implemented virtual signing room for providing access to at least one document by a plurality of users from a plurality of remote locations, comprising:

a document management module, for managing the at least one document, the document management module comprising a document-to-party mapping module for specifying access rights to the at least one document; and

a deal management module, coupled to the document management module, for maintaining a deal completion list containing document-related task items.

2. The virtual signing room of claim 1, wherein the at least one document is encoded in an extensible markup language (XML) format.

3. The virtual signing room of claim 1, wherein the document management module further comprises an audit module for tracking revisions to the at least one document.

4. The virtual signing room of claim 3, wherein the document management module further comprises a notification module for automatically notifying at least one user of a revision to the at least one document.

AMENDED CLAIMS

[received by the International Bureau on 13 September 2000 (13.09.00);
original claims 1 and 4 amended; new claims 5-50 added;
remaining claims unchanged (11 pages)]

What is claimed is:

1. A computer-implemented virtual signing room for providing access to at least one document by a plurality of users from a plurality of locations, comprising:

a document management module, for managing the at least one document;

a party-to-document mapping module for specifying access rights to the at least one document; and

a deal management module, coupled to the document management module, for maintaining a deal completion list containing document-related task items;

wherein the document management module permits access to the at least one document responsive to the party-to-document mapping module indicating that a user has access rights to the at least one document.

2. The virtual signing room of claim 1, wherein the at least one document is encoded in an extensible markup language (XML) format.

3. The virtual signing room of claim 1, wherein the document management module further comprises an audit module for tracking revisions to the at least one document.

4. The virtual signing room of claim 1, wherein the document management module accepts and applies a revision to the at least one document;

and wherein the document management module further comprises a notification module for automatically notifying at least one user of the revision.

5. The virtual signing room of claim 4, wherein the notification module notifies the at least one user of the revision by displaying a dialog box responsive to the user accessing the virtual signing room.

6. The virtual signing room of claim 4, wherein the notification module notifies the at least one user of the revision by transmitting an electronic mail message to the user.

7. The virtual signing room of claim 4, wherein the notification module retrieves an indicator specifying a notification medium for a portion of the document corresponding to the revision, and wherein the notification module notifies the at least one user of the revision via the specified notification medium.

8. The virtual signing room of claim 1, wherein the document management module accepts and applies a revision to the at least one document responsive the party-to-document mapping module indicating that a user has access rights permitting revision of the at least one document.

9. The virtual signing room of claim 1, wherein the party-to-document mapping module specifies access rights to a portion of at least one document.

10. The virtual signing room of claim 9, wherein the document management module further accepts a revision to the portion of the at least one document responsive to the party-to-document mapping module indicating that a user has access rights permitting revision of the portion.

11. The virtual signing room of claim 1, wherein the party-to-document mapping module specifies access rights to a first portion of a document and different access rights to a second portion of the document.

12. The virtual signing room of claim 1, wherein the party-to-document mapping module comprises:

a role identifier for defining a signing role for each of at least one user; and

a map, coupled to the role identifier, for associating each signing role with at least one document.

13. The virtual signing room of claim 12, wherein the role identifier comprises an authenticator for authenticating the identity of the at least one user, and for verifying the authority of the user to sign the document.

14. The virtual signing room of claim 13, wherein the authenticator authenticates the identity of the user by public key cryptography.

15. The virtual signing room of claim 13, further comprising:

a smartcard reader, coupled to the authenticator, for reading a private key from a smartcard provided by the at least one user;

and wherein the authenticator authenticates the identity of the user by validating the private key.

16. The virtual signing room of claim 13, wherein the authenticator authenticates the identity of the user by receiving and validating biometric data of the user.

17. The virtual signing room of claim 13, wherein the authenticator authenticates the identity of the user by receiving a passcode from the user and validating the received passcode.

18. The virtual signing room of claim 12, wherein the role identifier receives input from a user specifying a signing role.

19. The virtual signing room of claim 12, wherein the role identifier retrieves data from a stored cookie specifying a signing role.

20. The virtual signing room of claim 12, wherein the party-to-document mapping module further retrieves a list of documents available for signing by the at least one user, based on the defined signing role.

21. The virtual signing room of claim 20, further comprising:

a parser, coupled to the role identifier, for identifying at least one portion of the at least one document, to be signed by the at least one user;

and wherein the party-to-document mapping module retrieves the list of documents available responsive to the identification by the parser.

22. The virtual signing room of claim 1, wherein the deal completion list comprises document-related task items including at least one selected from the group consisting of:

at least one signature to be applied to a document;

at least one data item to be provided;

a deadline date for applying a signature to a document; and

a signing sequence for a document.

23. The virtual signing room of claim 1, wherein the deal management module further comprises a next step module for monitoring a current status and next step specified by the deal completion list.

24. The virtual signing room of claim 23, wherein the deal management module updates the deal completion list responsive to at least one selected from the group consisting of:

application of a signature to a document;

revision of a document;

deletion of a document; and

creation of a document.

25. The virtual signing room of claim 1, wherein the virtual signing room is accessible to at least one of the users over a network.

26. A computer-implemented collaborative document editing system, comprising:

a document management module, for managing at least one document;

an input device, for receiving user input specifying at least one revision to the at least one document;

a storage device, coupled to the document management module, for storing revision privileges for at least one user;

a party-to-document mapping module, coupled to the storage device, for retrieving revision privileges from the storage device;

a revision module, coupled to the input device, to the document management module, and to the party-to-document mapping module, for, responsive to the revision privileges permitting the user to edit the document, modifying the document according to the specified revision; and

an audit module, coupled to the revision module, for, responsive to the revision privileges permitting the user to edit the document, tracking the specified revision to the document.

27. The system of claim 26, wherein the storage device stores revision privileges corresponding to at least a portion of the at least one document.

28. The system of claim 26, further comprising a notification module, coupled to the audit module, for automatically notifying at least one user of a revision to the at least one document.

29. The system of claim 26, wherein the input device receives user input from a remote user over a network.

30. The system of claim 26, wherein the party-to-document mapping module comprises:

a role identifier for defining a role for each of at least one user; and

a map, coupled to the role identifier, for associating each role with at least one document;

and wherein each retrieved revision privilege corresponds to least one role.

31. The system of claim 30, wherein the role identifier comprises an authenticator for authenticating the identity of the at least one user, and for verifying the authority of the user to edit the document.

32. The system of claim 31, wherein the authenticator authenticates the identity of the user by public key cryptography.

33. The system of claim 31, further comprising:

a smartcard reader, coupled to the authenticator, for reading a private key from a smartcard provided by the at least one user;

and wherein the authenticator authenticates the identity of the user by validating the private key.

34. The system of claim 31, wherein the authenticator authenticates the identity of the user by receiving and validating biometric data of the user.

35. The system of claim 31, wherein the authenticator authenticates the identity of the user by receiving a passcode from the user and validating the received passcode.

36. The system of claim 26, wherein the party-to-document mapping module retrieves revision privileges for each of at least two portions of the document, and wherein the revision module modifies the document responsive to the revision privileges for a portion of the document corresponding to the specified revision permitting the user to edit the portion.

37. The system of claim 36, wherein each portion corresponds to a field.

38. The system of claim 26, further comprising an output device, coupled to the party-to-document mapping module;

wherein the party-to-document mapping module further retrieves viewing privileges for the at least one document;

and wherein, responsive to the viewing privileges for a document permitting the user to view the document, the output device outputs the document.

39. The system of claim 26, further comprising an output device, coupled to the party-to-document mapping module;

wherein the party-to-document mapping module further retrieves viewing privileges for at least a portion of the at least one document;

and wherein, responsive to the viewing privileges for a portion of a document permitting the user to view the portion, the output device outputs the portion.

40. The system of claim 39, wherein each portion corresponds to a field.

41. The system of claim 26, further comprising a check-in module, coupled to the document management module, for receiving at least one document from an off-line source.

42. The system of claim 26, wherein the input device accepts input specifying privileges for at least one document.

43. A computer-implemented method for collaborative document editing, comprising:

storing revision privileges for at least one user;

receiving user input specifying at least one revision to the at least one document;

retrieving revision privileges;

responsive to the revision privileges permitting the user to edit the document:

modifying the document according to the specified revision; and

tracking the specified revision to the document.

44. The method of claim 43, further comprising notifying at least one user of a revision to the at least one document.

45. The method of claim 43, further comprising:

defining a role for each of at least one user; and

associating each role with at least one document;

and wherein each retrieved revision privilege corresponds to least one role.

46. The method of claim 45, further comprising:

authenticating the identity of the at least one user; and

verifying the authority of the user to edit the document.

47. A computer program product comprising a computer-usable medium having computer-readable code embodied therein for collaborative document editing, comprising:

computer-readable program code configured to cause a computer to store revision privileges for at least one user;

computer-readable program code configured to cause a computer to receive user input specifying at least one revision to the at least one document;

computer-readable program code configured to cause a computer to retrieve revision privileges;

computer-readable program code configured to cause a computer to,

responsive to the revision privileges permitting the user to edit the document:

modify the document according to the specified revision; and

track the specified revision to the document.

48. The computer program product of claim 47, further comprising computer-readable program code configured to cause a computer to notify at least one user of a revision to the at least one document.

49. The computer program product of claim 47, further comprising:

computer-readable program code configured to cause a computer to define a role for each of at least one user; and

computer-readable program code configured to cause a computer to associate each role with at least one document;

and wherein each retrieved revision privilege corresponds to least one role.

50. The computer program product of claim 49, further comprising:

computer-readable program code configured to cause a computer to authenticate the identity of the at least one user; and

computer-readable program code configured to cause a computer to verify the authority of the user to edit the document.

STATEMENT UNDER PCT ARTICLE 19(1)

The above amendments to the Claims are being submitted in accordance with the Patent Cooperation Treaty Article 19.

The above-described amendments include the amendments made to the related U.S. case which is pending.

The above-described amendments do not go beyond the disclosure of the international application as filed, and entry of these amendments is respectfully requested.

Replacement sheets effecting the above-described amendments are being transmitted herewith.

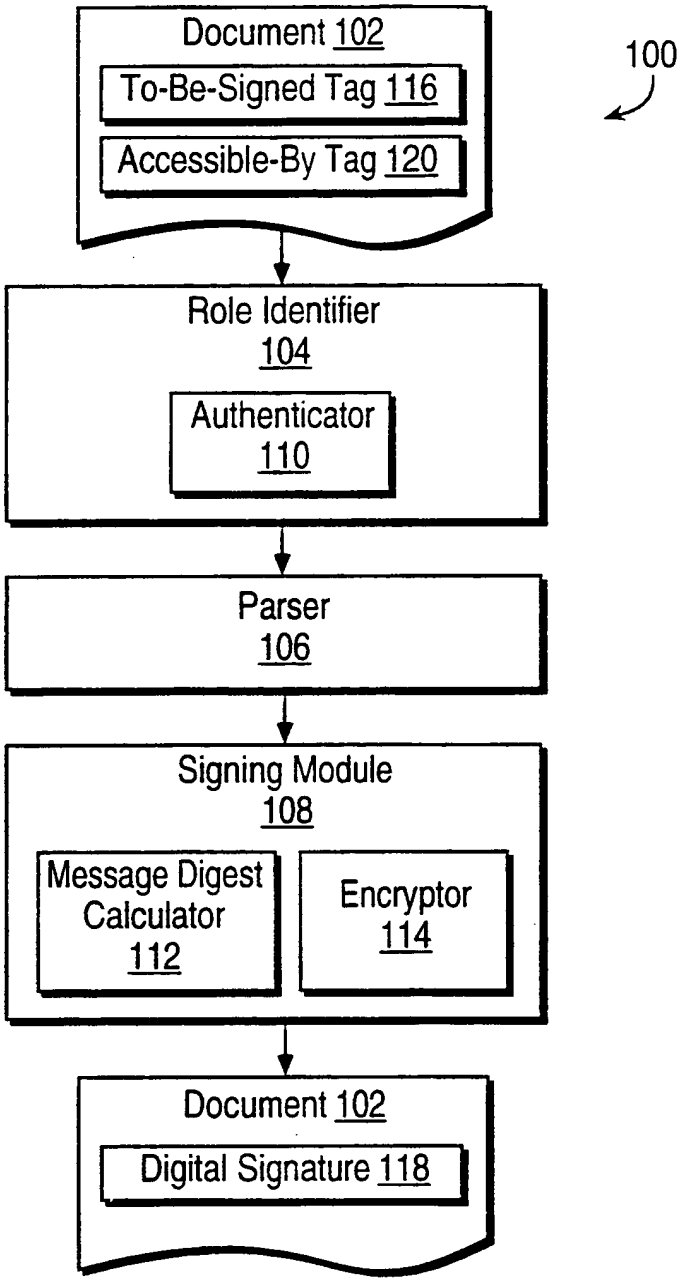

Document 102
To-Be-Signed Tag 116
Accessible-By Tag 120
100
Role Identifier
104
Authenticator
110
Parser
106
Signing Module
108
Message Digest
Calculator
112
Encryptor
114
Document 102
Digital Signature 118

FIG. 1

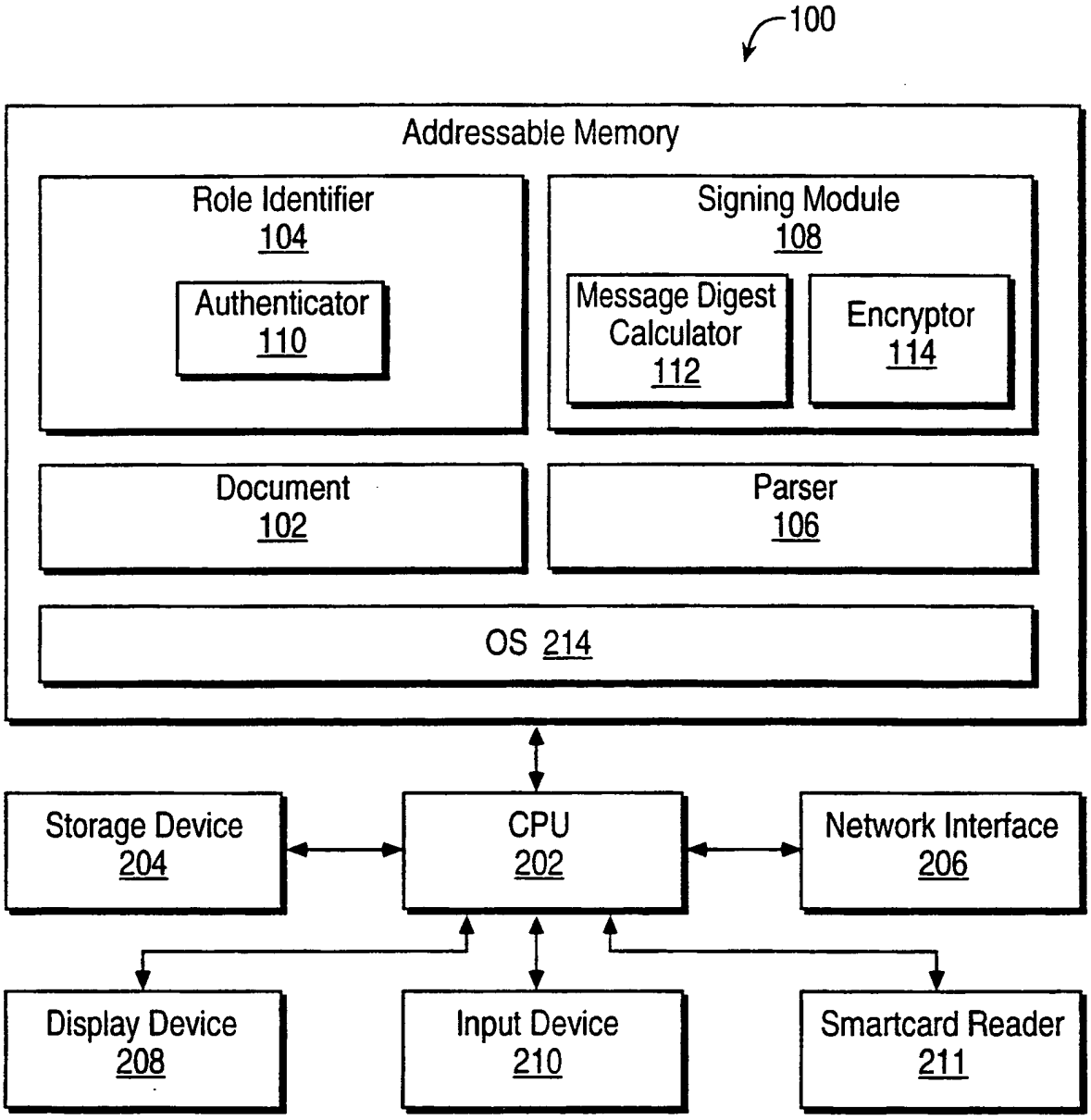
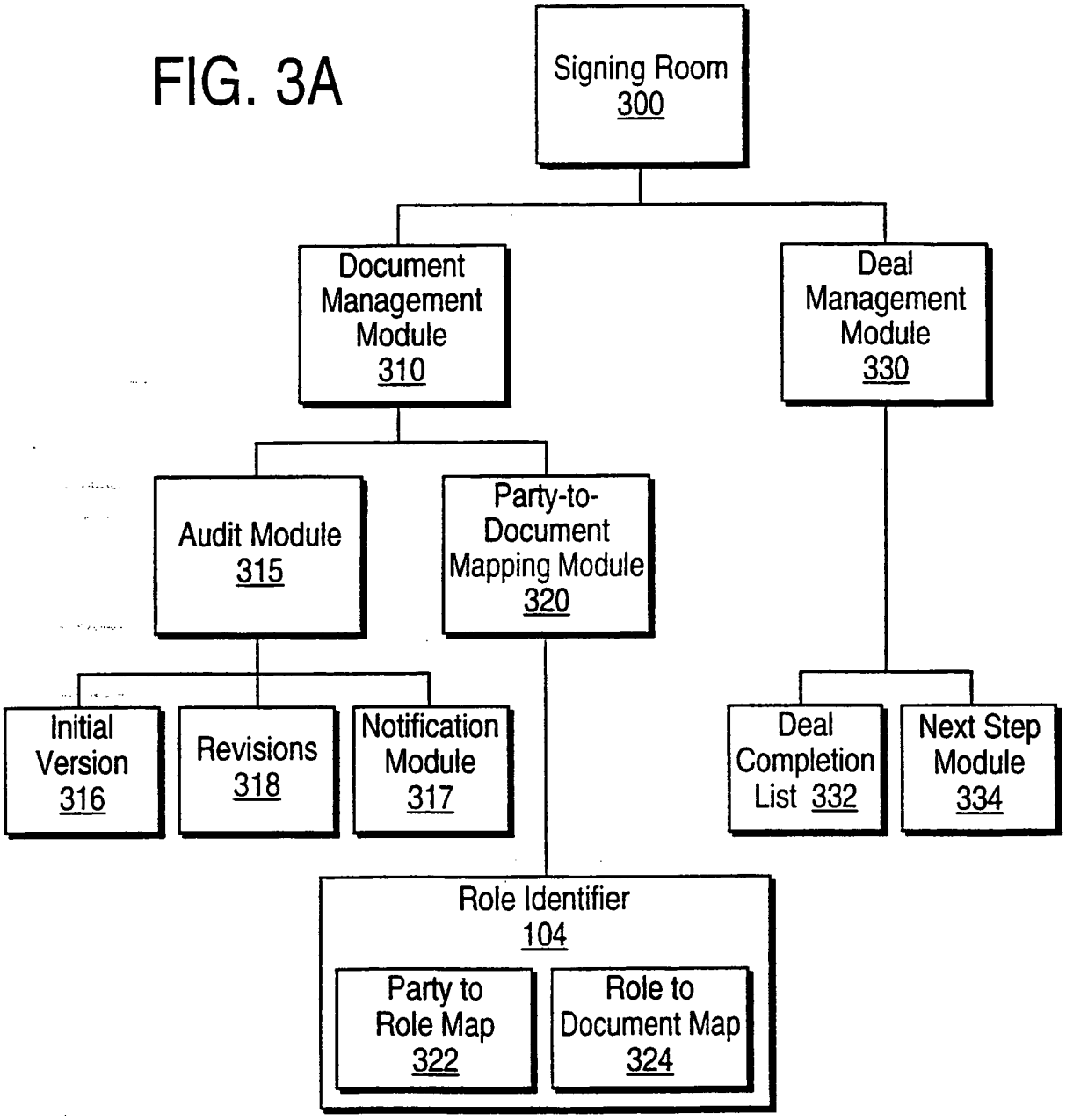

100
Addressable Memory
Role Identifier
104
Authenticator
110
Signing Module
108
Message Digest
Calculator
112
Encryptor
114
Document
102
Parser
106
OS 214
Storage Device
204
CPU
202
Network Interface
206
Display Device
208
Input Device
210
Smartcard Reader
211

FIG. 2

FIG. 3A


Signing Room
300
Document Management Module
310
Deal Management Module
330
Audit Module
315
Party-to-Document Mapping Module
320
Initial Version
316
Revisions
318
Notification Module
317
Deal Completion List
332
Next Step Module
334
Role Identifier
104
Party to Role Map
322
Role to Document Map
324

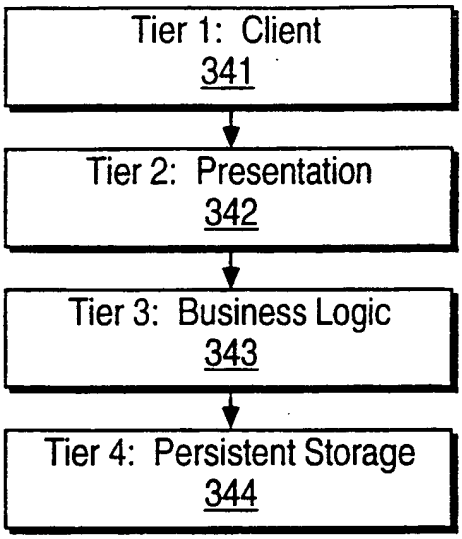

Tier 1: Client
341
Tier 2: Presentation
342
Tier 3: Business Logic
343
Tier 4: Persistent Storage
344

FIG. 3B

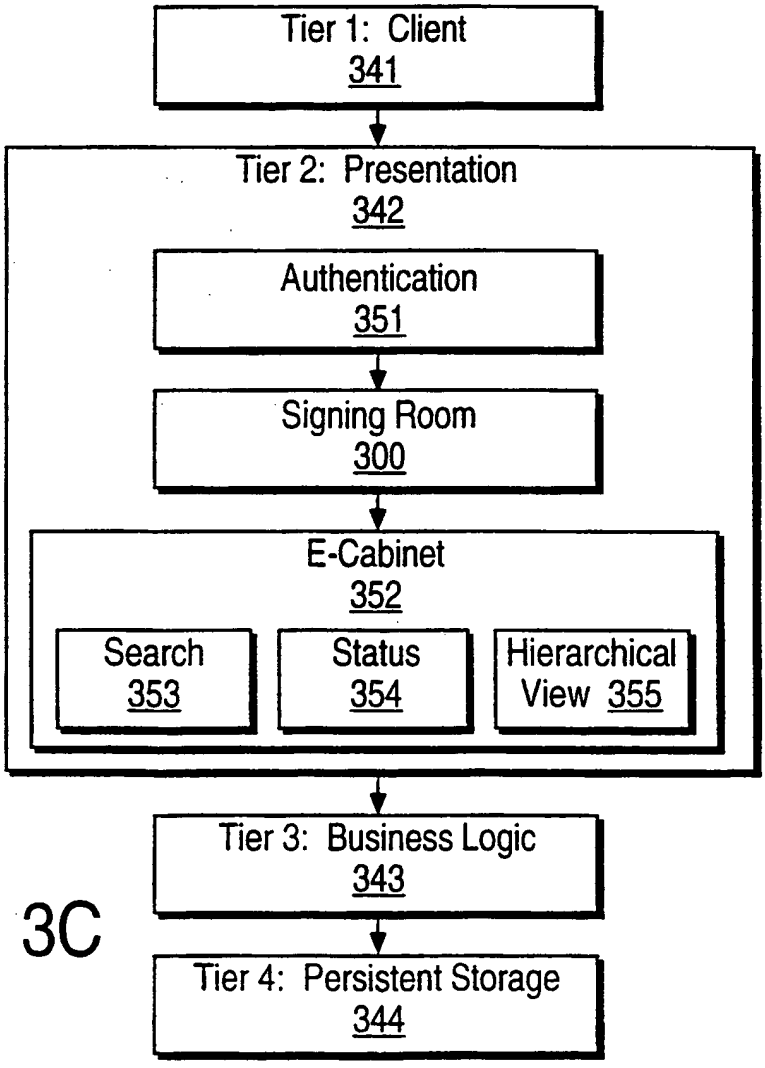

Tier 1: Client
341
Tier 2: Presentation
342
Authentication
351
Signing Room
300
E-Cabinet
352
Search
353
Status
354
Hierarchical
View 355
Tier 3: Business Logic
343
Tier 4: Persistent Storage
344

FIG. 3C

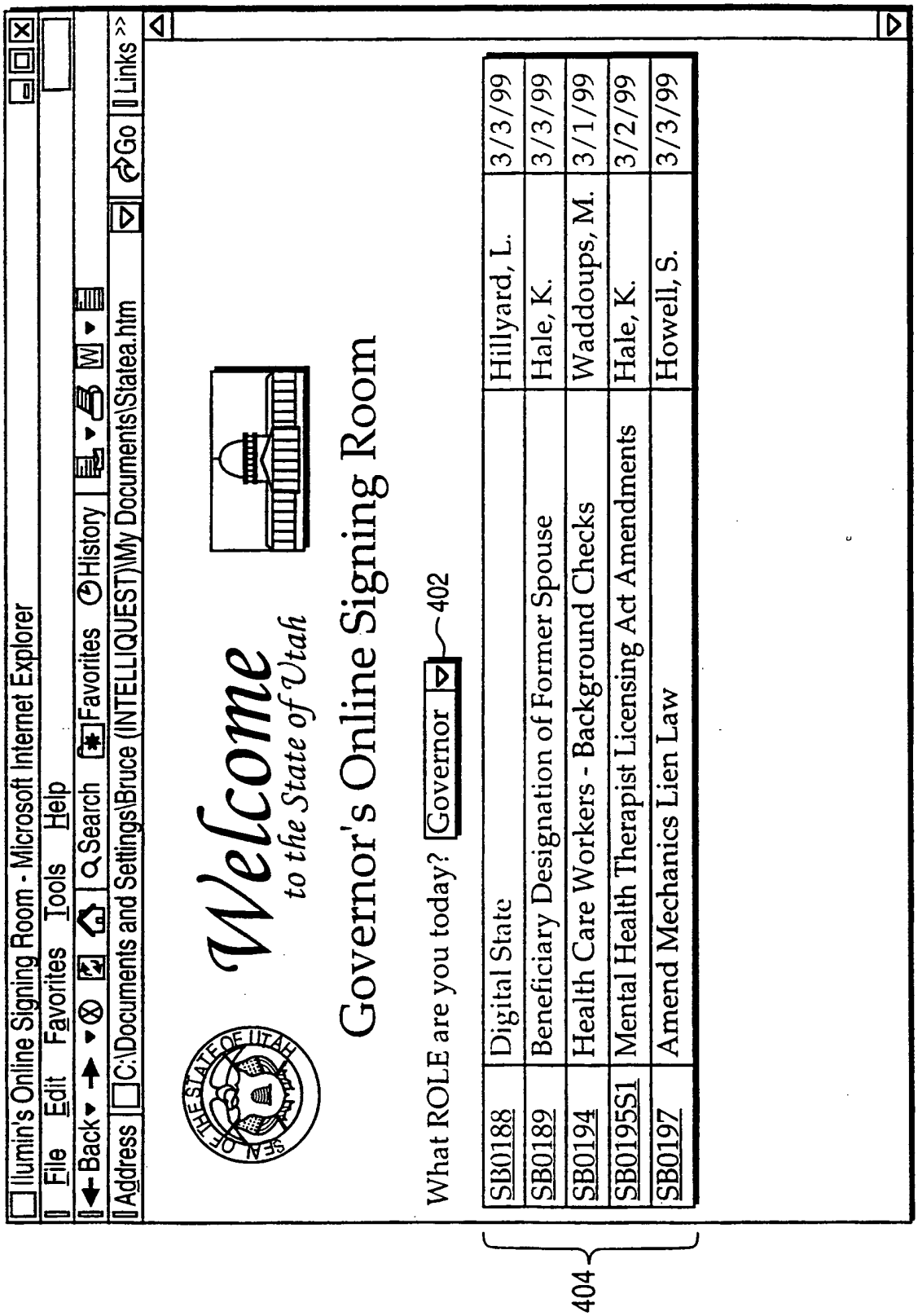

Illumin's Online Signing Room - Microsoft Internet Explorer
File Edit Favorites Tools Help
Back Search Favorites History
Address C:\Documents and Settings\Bruce (INTELLIQUEST)\My Documents\Statea.htm
Go Links
Welcome
to the State of Utah
Governor's Online Signing Room
What ROLE are you today? Governor
402
SB0188 Digital State Hillyard, L. 3/3/99
SB0189 Beneficiary Designation of Former Spouse Hale, K. 3/3/99
SB0194 Health Care Workers - Background Checks Waddoups, M. 3/1/99
SB0195S1 Mental Health Therapist Licensing Act Amendments Hale, K. 3/2/99
SB0197 Amend Mechanics Lien Law Howell, S. 3/3/99
404

FIG. 4A

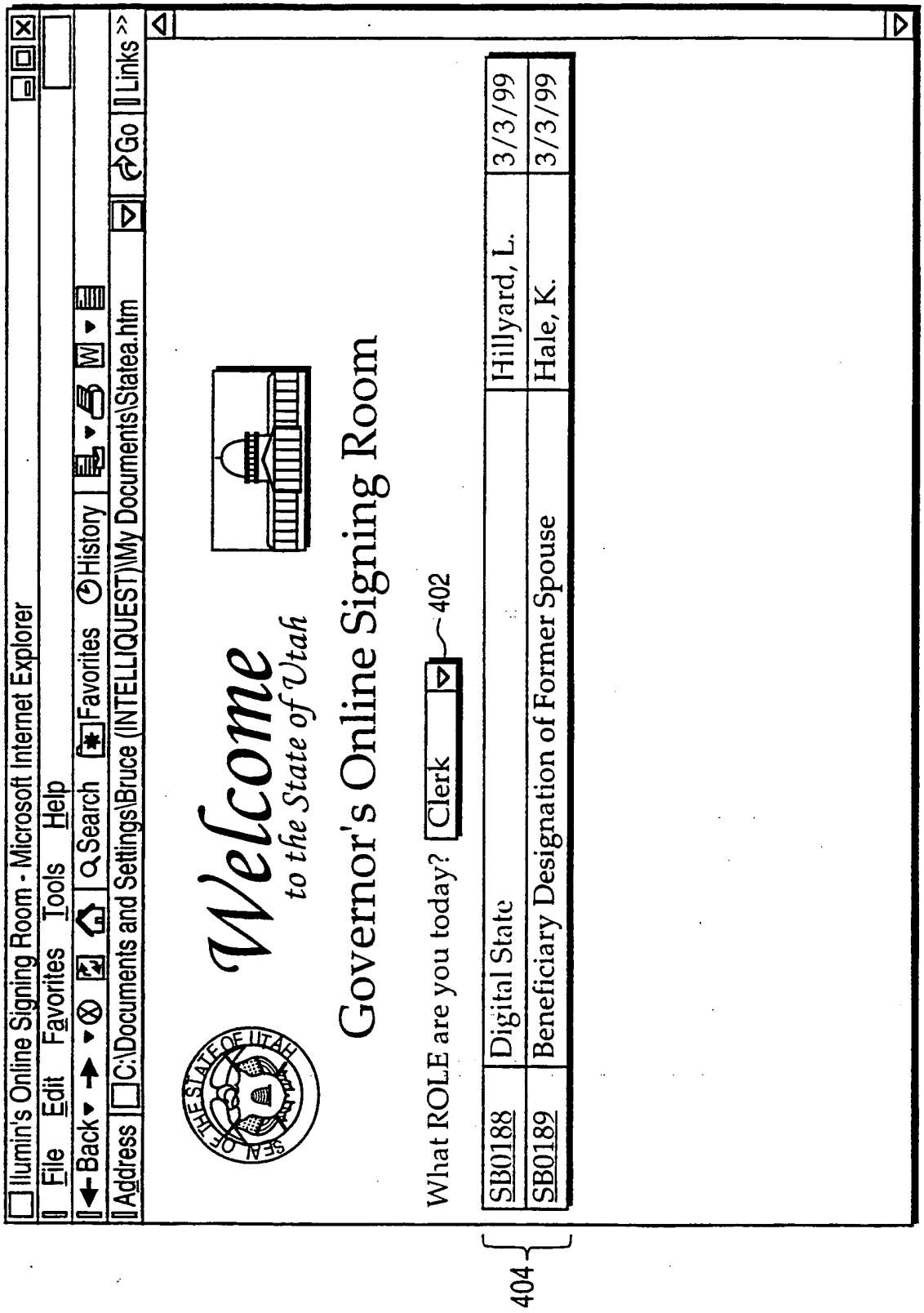

Ilumin's Online Signing Room - Microsoft Internet Explorer
File Edit Favorites Tools Help
Back Search Favorites History
Address C:\Documents and Settings\Bruce (INTELLIQUEST)\My Documents\Statea.htm
Go Links >>
Welcome
to the State of Utah
Governor's Online Signing Room
What ROLE are you today? Clerk
402
SB0188 Digital State Hillyard, L. 3/3/99
SB0189 Beneficiary Designation of Former Spouse Hale, K. 3/3/99
404

FIG. 4B

500

U.S. Distributor Application & Agreement

Personal Information (Please print) *Required Information ~ 503 501

Businesses must also fill out a Business Application Addendum (See instructions on back)

*Applicant's Name or Company Name (Last, First, Middle Initial use second line if necessary)

Applicant's Name or Company Name (Continued) 501

*Applicant: ☐Social Security Number ☐Federal ID Number (Business Addendum required)

Spouse (or Co-Applicant's Name)

Spouse (or Co-Applicant): ☐Social Security Number ☐Federal ID Number

*U.S. Mailing Address

*City, State, Zip Code

*U.S. Shipping Address (Note: UPS will not deliver to P.O. Box Numbers)

*U.S. Shipping Address (Continued)

*City, State, Zip Code

*Date of Birth (Month/Day/Year)

*Daytime Phone (Please Include Area Code)

*Alternate Phone (Please include Area Code)

*Evening Phone (Please include Area Code)

Cellular Phone (Please include Area Code)

Fax (Please include Area Code)

E-mail address (if any i.e. *yourname@serviceprovider.com*)

*Personal Sponsor's Information ~ 504

The distributor that referred you to the company. Placement and personal sponsors may be the same (see instructions on reverse side).

Personal Sponsor's Name (Last, First, Middle Initial)

Personal Sponsor's Phone (Please Include Area Code)

Personal Sponsor's ID Number

FIG. 5A-1

FIG. 5A

FIG. 5A-1	FIG. 5A-3
FIG. 5A-2	FIG. 5A-4

500

Placement Information ←505

The distributor that you are placed directly under. Placement sponsor must be in the downline of your Personal sponsor. It is highly recommended that you ***NOT*** fill out placement information upon sign-up. Leaving it blank will give your personal sponsor 120 days to determine where to place you using a placement sponsor change form. This is your one placement. If you are placed anywhere other than your Personal Sponsors first level, you cannot be moved.

Placement Sponsor's Name (Last, First, Middle Initial)

Placement Sponsor's Phone (Please Include Area Code) Placement Sponsor's ID Number

*Sign-up fee – non-refundable (Amount $20.00-Complimentary Starter-Kit included) ←506

METHOD OF PAYMENT: ☐Credit card (fill out below) ☐ACH ☐Check ☐Cash ☐Money Order

Credit Card Number ☐VISA ☐M/C ☐DISCOVER Exp Date (month/year)

Name on Card (exactly as it appears)

X ←502

Authorized Signature

Make checks and money orders payable to Morinda, Inc.
Return this form and $20.00 plus local sales tax and shipping for your Starter Kit to: Morinda, Inc. ATTN: Distributor Services P.O. Box 4000, Orem, UT 84059

If you have prepaid for the Starter Kit place validation sticker here.

FIG. 5A-2

500

Case AutoShip Program Information ←507 Please refer to instructions on the back

☐ Enroll me in Morinda's Case AutoShip Program. (If checked, fill out payment information below) I understand that I may order any products from Morinda's Case AutoShip Catalog to meet this requirement. I further understand that in order to fully qualify as a Case AutoShip Distributor, my orders for the month must equal or exceed 120 QPV.

Note: Orders from Morinda's Case AutoShip Catalog, *must be made prior to the 15th of each month*. If your orders made prior to that date do not equal 120 QPV, you will automatically be sent 1 case (4 bottles) of TAHITIAN NONI® Juice.

☐ I prefer Kosher TAHITIAN NONI® juice. I understand that the cost of Kosher TAHITIAN NONI® juice is $124.00 per case.

☐ I would like my case of TAHITIAN NONI® juice regardless of any other purchases. (If checked, fill out payment information below)
I authorize Morinda® to send me _____ case(s) of TAHITIAN NONI® juice OR _____ case(s) of Kosher TAHITIAN NONI® juice each month regardless of any other purchases made under my ID Number during any month.

Hawaii, Puerto Rico, and Alaska only
Please check one of the following:
☐ I will pick up my AutoShip from a local warehouse
☐ I would like my AutoShip delivered to my shipping address

AutoShip Payment Information ←508

METHOD OF PAYMENT: ☐Credit card ☐CASH (Must be accompanied by Cash AutoShip Voucher)
☐ACH (Voided check must be accompanied by an ACH authorization form)

Credit Card Number ☐VISA ☐M/C ☐DISCOVER Exp Date (month/year)

Name on Card (exactly as it appears)

Billing Address

City, State, Zip Code

X ←502
Authorized Signature

FIG. 5A-3

500

Nonresident Alien Distributors ←509

☐ I am now living in the United States, but am no a U.S. citizen
Nonresident Aliens in the U.S. are required by law to submit an IRS Form W-8

Order and Sign-up numbers ←510

U.S. English . . . . 1-800-445-2969 Spanish 1-800-445-8933
Tahiti Dream . . . . 1-888-588-8244 Chinese 1-888-545-0304

*Signature (Required) ←511

The undersigned hereby applies to become an independent distributor of Morinda, Inc. As an independent distributor, I agree to the terms and conditions contained on the reverse side of this Distributor Application and Agreement and in the Morinda Distributor Manual.

X ←502
Authorized Signature Date

X ←502
Spouse (or Co-Applicant Signature) Date

for office use only:
entered by:_____ Date:_____
checked by: _____ Date:_____

Distributor ID# ~512

FIG. 5A-4

500

TERMS AND AGREEMENT:

Distributor and Morinda Inc. (Morinda) hereby agree to the following terms and conditions:

1. **Legal Age**. Distributor is of legal age to enter into this Application and Agreement (the "Agreement") in the state in which Distributor resides.

2. **Acceptance**. This Agreement shall be effective upon acceptance by Morinda at its place of business in Provo, Utah. Distributor may buy products at wholesale from Morinda. Morinda reserves the right, in its sole discretion, to decline to accept any Agreement. Upon Company's acceptance of this Agreement, Distributor shall have the right to sell products and services of Morinda and to participate in its Compensation Plan.

3. **Term**. Subject to the provisions of Section 16, this Agreement shall have a term beginning on the date of acceptance by Morinda and ending one year from the date thereof (the "Anniversary Date") unless renewed by Distributor prior to the Anniversary Date. Morinda shall have the right to decline, in its sole discretion, any renewal application by Distributor. The right to renew this Agreement or the failure to do so is subject to the terms and provisions of the Distributor Manual.

4. **Independent Contractor Status**. Distributor understands that Distributor is an independent contractor and not an employee, agent, franchisee, joint venturer, partner or owner of Morinda. Distributor is solely responsible for compliance with any and all laws or regulations related to its business in any jurisdiction exercising authority over said business, including but not limited to the duty to license its business and to comply with all other regulations. Distributor will obey any and all Federal or local laws, statutes and regulations applicable to said business. Distributor has no authority to bind Morinda or incur any obligation on behalf of Morinda.

5. **Responsibility for Taxes**. Distributor has no authority to bind Morinda or incur any obligation on behalf of Morinda. See Distributor Manual.

6. **Sales and Use Taxes**. To ensure compliance with the sales and use tax requirements of each state, unless otherwise mandated by state law, Morinda shall collect and remit all applicable sales and use taxes on products based upon the suggested retail price of the product. The applicable rate of tax due shall be based on the address to which the product and/or material is shipped.

7. **Compensation**. Distributor understands that any compensation Distributor receives from Morinda is related primarily to the sale of products and services to non-participants, and that there is no compensation for sponsoring. Distributor understands that Distributor is not guaranteed any income, profits or success and certifies that no such representations have been made to Distributor either by Morinda or any other Distributor. Distributor shall make no claims or representations of actual or potential earnings, guaranteed or anticipated profits or sales success. Distributor agrees to sell or consume at least 70% of product previously purchased by Distributor and agrees not to make retail sales.

8. **No Other Purchase**. In order to become a Distributor and begin the business, Distributor is not required to make any purchase other than the sign-up fee, which includes a Distributor Kit. The purchase of a Distributor Kit is optional in the State of North Dakota. In order to comply with the Direct Selling Associations (the "DSA") Code of Ethics, the kit must be refundable in accordance with the terms of the DSA refund policy.

9. **Refunds**. Distributor agrees to abide by Morinda's retail customer refund policy, as set forth in the Distributor Manual. "Distributor is eligible to receive a refund for products, services and literature purchased, less a 10% handling fee if Distributor chooses to terminate the Agreement and return products or services in currently marketable condition within twelve (12) months of purchase in accordance with the terms set forth in their Distributor Manual." All other refunds for returned product will be dealt with as outlined in the Distributor Manual. See Distributor Manual for all provisions.

FIG. 5B-1

10. **Proprietary Rights/Use of Company Materials**. Distributor agrees not to use proprietary trade names, trademarks or other copyrighted materials of Morinda without the prior written consent of Morinda. Morinda and its affiliated entities have proprietary rights to its distributor network and lists of distributor names and other confidential business and financial information of Morinda. Distributor will not use any Morinda networks, distributor lists, or other confidential information to promote the sale or use of any products or services, other than those offered through Morinda and only in compliance with the terms of this agreement and the Distributor Manual. Distributor agrees that any unauthorized disclosure of such confidential information, including to Distributor's spouse if not a co-applicant, shall constitute a material breach of this Agreement. Distributor further agrees not to hold a beneficial interest in more than one Morinda distributorship as outlined in the Distributor Manual.

11. **Non-Solicitation**. As an inducement for Morinda to enter into this Agreement and in consideration of the mutual covenants contained herein, Distributor agrees that during the term of this Agreement and for a period of one (1) year thereafter, Distributor shall not, directly or indirectly, on his or her own behalf or on the behalf of any other person or entity, solicit, induce, or hire or attempt to solicit, induce or hire any Distributor, employee, member, customer, supplier or vendor of Morinda (i) to enter into any business relationship with any individual or company which sells products or services which compete with the products and/or services of Morinda, or (ii) to terminate or alter his or her business or employment relationship with Morinda.

12. **Training**. In the event Distributor sponsors other distributors, Distributor agrees to perform a bonafide supervisory, distributive and selling function in connection with the sale of Morinda's goods and services to the ultimate consumer.

13. **Cross Selling/Cross Sponsoring**. See Distributor Manual

14. **No Exclusive Territory**. Distributor understands that no exclusive territory is granted by this Agreement, nor does this Agreement constitute the sale of a security or a franchise.

15. **Assignability**. Distributor understands and agrees that this Agreement may not be transferred or assigned without the prior written approval of Morinda, in its sole discretion, and then only in accordance with the distributor Manual. Morinda may assign this agreement at any time.

16. **Termination**. (a) DISTRIBUTOR ACKNOWLEDGES THAT HE OR SHE IS FREE TO TERMINATE THIS AGREEMENT AT ANY TIME FOR ANY REASON upon written notice to Morinda. Morinda may terminate this Agreement at any time upon thirty (30) days written notice for any reason, and may terminate immediately for violation of the policies in the Distributor Manual. Where state laws on termination are inconsistent with this provision, then the applicable state law shall apply. Immediately upon termination of this Agreement, Distributor shall, (a) lose all rights to purchase products from Morinda at distributor cost; (b) shall cease from representing himself or herself as a distributor of Morinda; (c) all rights to his or her distributorship, his or her participation and position in the Compensation Plan, including all future commissions and earnings resulting therefrom; and (d) take all other actions reasonably required by Morinda relating to protection of Morinda's confidential information, including the discontinuance of Morinda's trademarks and service marks.

17. **Amendment**. Distributor understands that Morinda may amend this Agreement, the Distributor Manual, prices for product, company literature and/or the Compensation plan, without prior notice, at any time, effective upon publication or transmittal of such amendment in official Company publications, literature or voice mail, as applicable. In the event of any conflict between the terms of this Agreement, the Rules and Regulations, the Distributor Manual or any other document and such amendment, the amendment shall control.

18. **Arbitration**. Distributor understands and agrees that except as set forth in the Manual, all claims and disputes relating to this Agreement, the rights and obligations of the parties or any other claims or causes of actions relating to the performance of either party under this Agreement and/or Distributor's purchase of products shall be settled totally and finally by arbitration in the City of Provo, State of Utah, in accordance with the Federal Arbitration Act and the Commercial Rules of the American Arbitration Association. This agreement is executed in Utah County, Utah and is governed by the laws of the State of Utah.

FIG. 5B-2

500

19. **Indemnification/Offset**. Distributor agrees to indemnity and hold harmless Morinda, its subsidiaries, affiliates and their shareholders, officers, agents, employees, and directors, from and against any claim, demand, liability, loss, cost or expense, including, but not limited to, court costs or attorneys' fees, asserted against or suffered or incurred by any of them by reason of, directly or indirectly, arising out of or in any way related to or connected with, allegedly or otherwise, the Distributor's: (a) activities as a distributor; (b) breach of the terms of this Agreement; or (c) violation of or failure to comply with any applicable federal, state or local law or regulation. Morinda shall have the right to offset any amounts owed by Distributor to Morinda (including, without limitation, the repayment of commissions as a result or product returns) against the amount of any commissions or bonuses or other monies owed to the Distributor.

20. **Liquidated Damages**. Distributor agrees that the liability of Morinda, and its officers, directors, and shareholders to Distributor for any claim whatsoever related to the relationship of Morinda and Distributor, including any cause of action in contract, tort, or strict liability, shall not exceed, and be limited to, the amount of unsold product inventory owned by Distributor, if any commissions at the time of the controversy or termination, if any, owed to Distributor. In no event shall Morinda be liable to Distributor for any incidental, special, exemplary, or consequential damages.

21. **Cumulative Remedies/Waiver**. All rights, powers and remedies given to Morinda are cumulative, not exclusive and in addition to any and all other rights and remedies provided by law. No failure or delay of Morinda to exercise any power or right under this Agreement or to insist upon strict compliance by Distributor with any obligation or provision, and no custom or practice of the parties at variance with this agreement shall constitute a waiver of Morinda's right to demand exact compliance therewith. Waiver by Morinda can be effective only in writing by an authorized officer of Morinda. The waiver by Morinda of any particular default by Distributor shall not affect or impair Morinda's rights with respect to any subsequent default, nor shall it affect in any way the rights or obligations of any Distributor.

22. **Survival**. The covenants and obligations of Distributor to protect the trade secrets and confidential information of Morinda, including, without limitation, those obligations and covenants contained in 10 and 11, shall survive termination of this agreement.

23. **Entire Agreement**. This Agreement, the Distributor Manual, and the Compensation Plan (all of which are incorporated herein by reference), constitute the entire Agreement between Distributor and Morinda, and no other promises, representations, guarantees, or agreements of any kind that are not otherwise made in accord with #17 above, shall be valid unless in writing and signed by both parties.

24. **Collection Fees**. Distributor is responsible for any and all collection fees due to any type of payment that is returned and a collection effort is made. Distributor understands that commissions earned will be held and could be applied to balance owing.

25. **Non-Resident Alien**. Those who are living in the United States who are not U.S. Citizens must submit the W-8 Certificate of Foreign Status Form. This can be obtained by calling 1-800-829-3676.

26. **Sponsor Changes**. By signing this application, Distributor's Personal Sponsor may change the Placement Sponsor within 120 days of sign-up without an additional signature.

27. **Severability**. If under any binding law or rule of any applicable jurisdiction, any provision of this Agreement is held to be invalid or unenforceable, Morinda, shall have the right to modify the invalid or unenforceable provision, or any portion thereof, to the extent required to be valid and enforceable. Distributor shall be bound by any such modification which shall be effective only in the jurisdiction in which it was required.

512

FIG. 5B-3

500

Distributor Application instructions

- Please make all information legible and complete.
- If pertinent information is left incomplete this application will be rejected.
- This hard copy will always be the determining factor if any discrepancies arise except in the case of sponsorship.
- If you have signed up over the phone previous to sending in this Distributor Application, sponsorship should not be different from the phone sign-up.
- Phone-in applicants must submit completed Distributor Application within 30 days. Failure to do so will put distributor status on hold and no commissions will be paid. If you have signed up over the phone previous to sending in this Distributor application, sponsorship should not be different.

Personal Information

- When signing up as a company name, a Business Application Addendum must be filled out in addition to this form, with the signatures of all parties in the company included. See the Distributor Manual for a copy of this form.
- The S.S./Federal ID# is absolutely required and must be the number corresponding to the distributorship. For corporations, partnerships, and trusts please submit all required documents as listed in the Distributor Manual.
- Having a co-applicant is optional. It is highly recommended that the spouse information be filled out as the spouse is considered as having a beneficial interest in the distributorship.
- Shipping address: we must have a second address for shipping if your mailing address is a PO Box, or if you would like your AutoShip sent to an alternate address.
- Birthday: This is needed as verification that the new distributor is of legal age to be a distributor in the state of their residency.
- Phone Number: Please indicate the numbers where you may be reached.

Personal Sponsor

Your personal Sponsor is the distributor that referred you the company.

- *Note: Your placement and personal sponsor may be the same distributor if you are on the personal sponsor's first level and have not been placed.*

Placement Sponsor

The distributor that you are placed directly under. Placement sponsor must be in the downline of your Personal sponsor. It is highly recommended that you *NOT* fill out placement information upon sign-up. Leaving it blank will give your personal sponsor 120 days to determine where to place you using a placement sponsor change form. This is your one placement. If you are placed anywhere other than your Personal Sponsors first level, you cannot be moved.

Starter Kit

A complimentary starter kit is sent out when you pay the sign-up fee.

FIG. 5B-4

500

The AutoShip Program

The AutoShip Program is specially designed for our distributors to:

1. Ensure that their personal monthly volume is met.
2. Make them eligible for all bonuses and commissions.
3. Conveniently receive product each month without having to call in and place an order.

Distributors must understand that at the time of AutoShip enrollment they are required to purchase 120 QPV

Hawaii, Puerto Rico, Alaska, and Guam

Distributors in Hawaii, Puerto Rico, Alaska, or Guam have the option of receiving their AutoShip order at their residence, or pick it up at the warehouse. You must specify this information on your original Distributor Application: otherwise it will be shipped directly to your residence.

Payment

If using someone else's Credit Card to pay for your AutoShip Order, you must have written consent from the cardholder in order for your AutoShip Agreement to be honored. For all those who wish to pay with an automatic check withdrawal, two things must be submitted:

1. Completed ACH authorization form.
2. Pre-printed voided check.

514

FIG. 5B-5

U.S. Distributor Application & Agreement

Personal Information (*Required Information)

600

Applicant's Name [*Last, First, Middle] 601

Applicant's SS Number [*nnn-nn-nnn] [Note] 604, 601

Spouse (or Co-Applicant's Name) [Last, First, Middle] [Note] 604, 601

Spouse (or Co-Applicant's) SSN [nnn-nn-nnn] 601

U.S. Mailing Address [*] [Note] 604, 601

City, State, Zip Code [*] [CA] [*nnnnn-n] 601

Date of Birth [JAN] [01], 19[0][0] [Note] 604, 601

Daytime Phone [*nnn-nnn-n] [Note] 604, 601

Alternate Phone [*nnn-nnn-n] 601

Evening Phone [*nnn-nnn-n] 601

Cellular Phone [nnn-nnn-n] 601

FAX [nnn-nnn-n] 601

E-Mail Address [ ]

[Generate Keys] [Explain] 603, 602

***Personal Sponsor's Information** The distributor that referred you to the company. Placement and personal sponsors may be the same. [Note] 604

Name [*Last, First, Middle] 601

Phone [nnn-nnn-nn] 601

ID Number [nnnnnnn] 601

Placement Information It is highly recommended that you *NOT* fill out placement information upon sign-up [Note] 604

Name [Last, First, Middle] 601

Phone [nnn-nnn-nn] 601

ID Number [nnnnnnn] 601

FIG. 6A

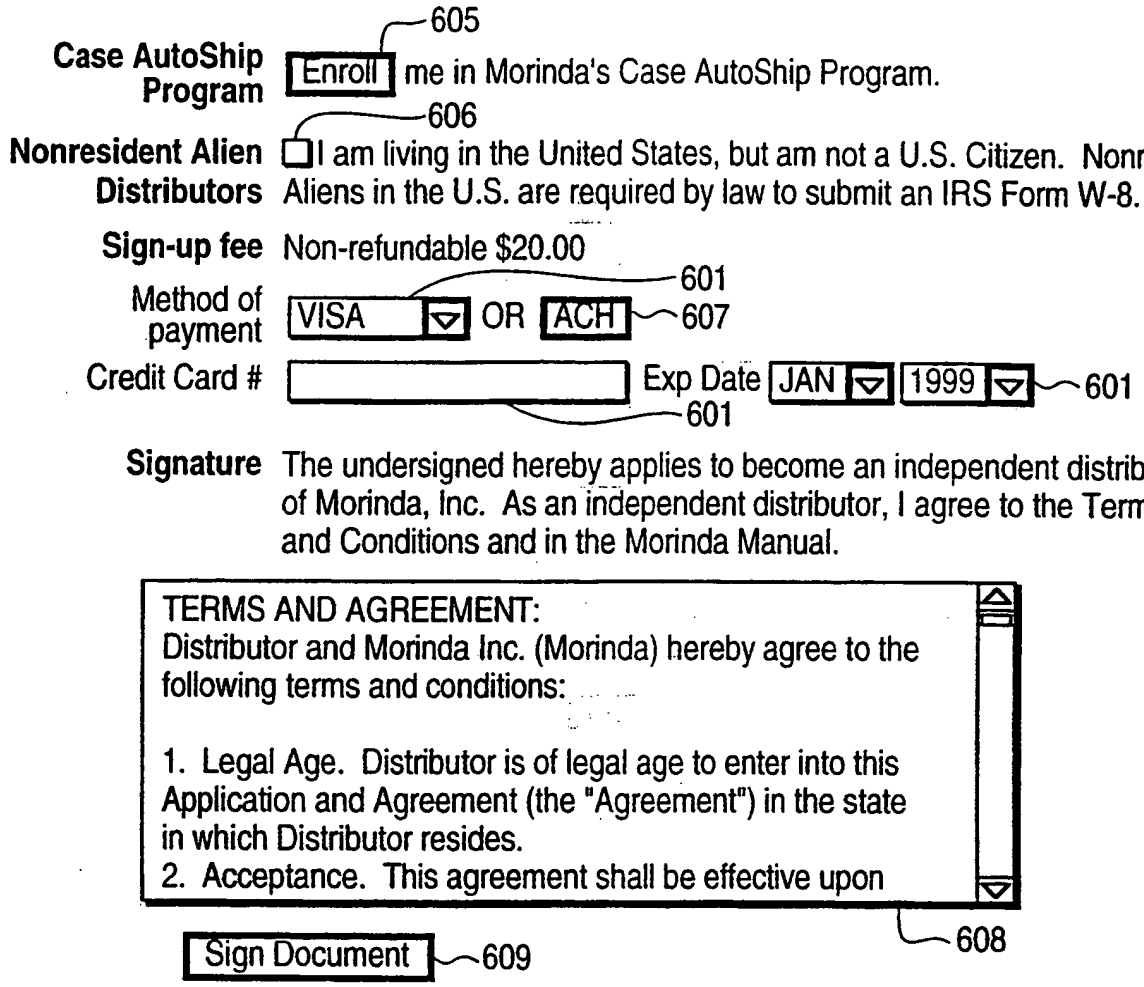

605
Case AutoShip Program
Enroll
me in Morinda's Case AutoShip Program.
606
Nonresident Alien Distributors
I am living in the United States, but am not a U.S. Citizen. Nonresident Aliens in the U.S. are required by law to submit an IRS Form W-8.
Sign-up fee
Non-refundable $20.00
601
Method of payment
VISA
OR
ACH
607
Credit Card #
Exp Date
JAN
1999
601
601
Signature
The undersigned hereby applies to become an independent distributor of Morinda, Inc. As an independent distributor, I agree to the Terms and Conditions and in the Morinda Manual.
TERMS AND AGREEMENT:
Distributor and Morinda Inc. (Morinda) hereby agree to the following terms and conditions:
1. Legal Age. Distributor is of legal age to enter into this Application and Agreement (the "Agreement") in the state in which Distributor resides.
2. Acceptance. This agreement shall be effective upon
608
Sign Document
609

FIG. 6B

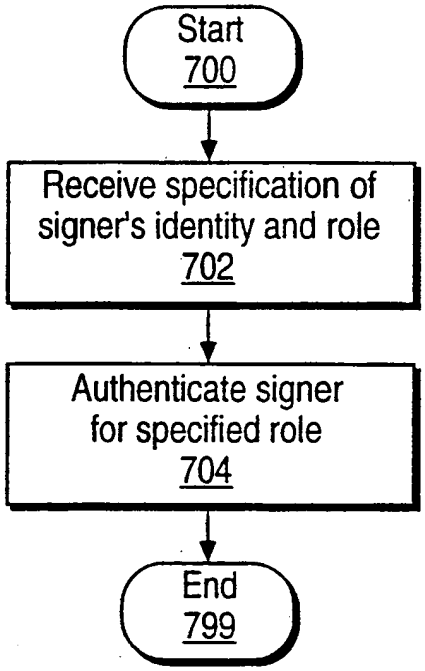
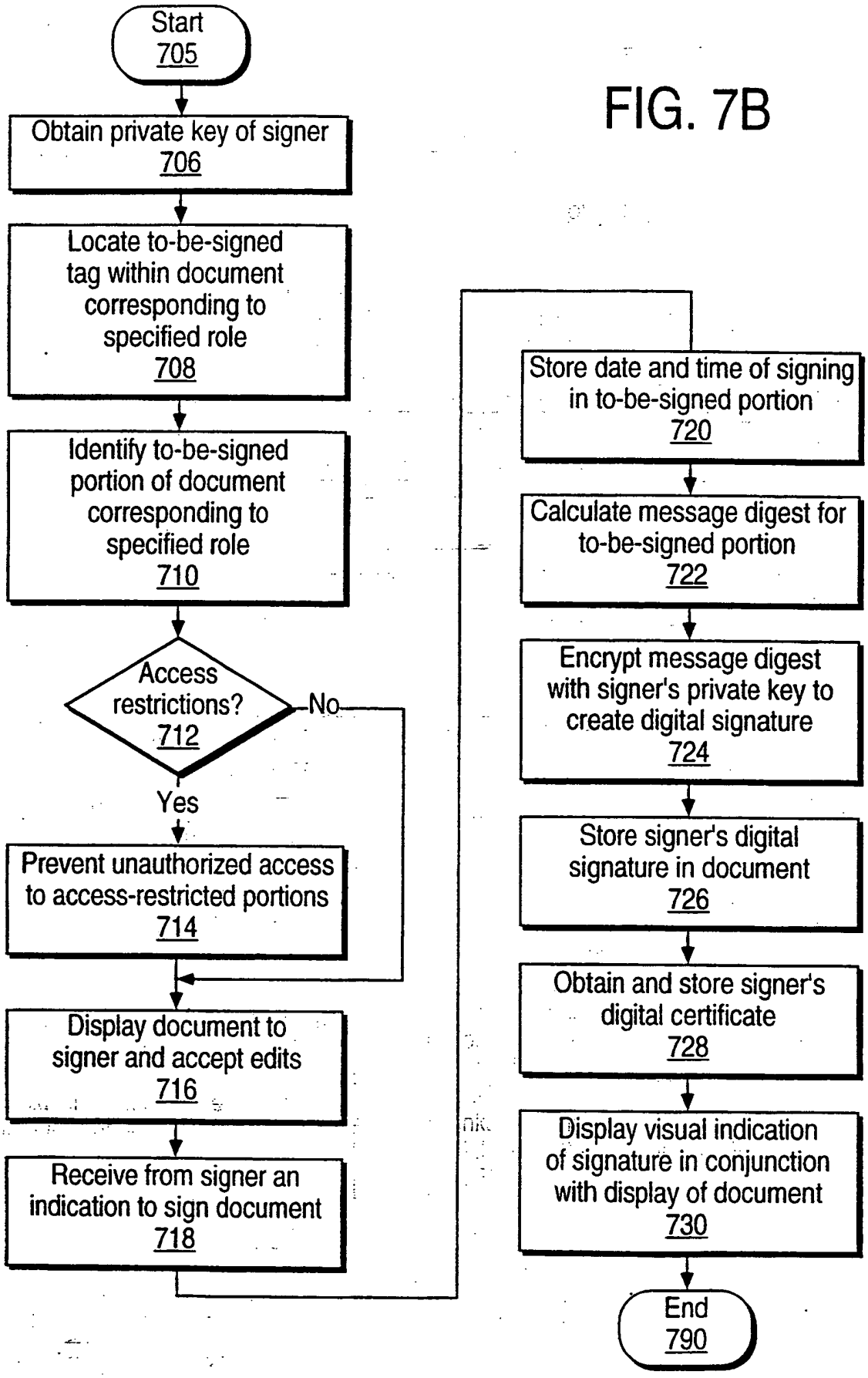

Start
700
Receive specification of signer's identity and role
702
Authenticate signer for specified role
704
End
799

FIG. 7A

FIG. 7B


Start
705
Obtain private key of signer
706
Locate to-be-signed tag within document corresponding to specified role
708
Identify to-be-signed portion of document corresponding to specified role
710
Access restrictions?
712
No
Yes
Prevent unauthorized access to access-restricted portions
714
Display document to signer and accept edits
716
Receive from signer an indication to sign document
718
Store date and time of signing in to-be-signed portion
720
Calculate message digest for to-be-signed portion
722
Encrypt message digest with signer's private key to create digital signature
724
Store signer's digital signature in document
726
Obtain and store signer's digital certificate
728
Display visual indication of signature in conjunction with display of document
730
End
790

U.S. Distributor Application & Agreement

800

Personal Information	(*Required Information)
Applicant's Name	BROWN, CHARLIE ~801
Applicant's SS Number	123-45-6789 ~801
Spouse (or Co-Applicant's Name)	QUEUE, SUZIE ~801
Spouse (or Co-Applicant's) SSN	987-65-4321 ~801
U.S. Mailing Address	8080 Yellow Brick Road ~801
City, State, Zip Code	UTOPIA UT 12345-4321 ~801
Date of Birth	FEB 01, 1952 ~801
Daytime Phone	123-555-4321 ~801
Alternate Phone	
Evening Phone	123-555-1234 ~801
Cellular Phone	123-555-5678 ~801
FAX	123-555-8765 ~801
E-Mail Address	chuck@mars.com
***Personal Sponsor's Information**	The distributor that referred you to the company. Placement and personal sponsors may be the same. Note ~604
Name	AUSTEN, JANE } 801
Phone	101-555-6166 } 801
ID Number	11223344 } 801
Placement Information	It is highly recommended that you *NOT* fill out placement information upon sign-up Note ~604
Name	
Phone	
ID Number	

FIG. 8A

806

Nonresident Alien Distributors no I am living in the United States, but am not a U.S. Citizen. Nonresident Aliens in the U.S. are required by law to submit an IRS Form W-8.

Sign-up fee Non-refundable $20.00

Method of payment VISA 802

Credit Card # 1234-xxxxx-xxxx Exp Date Jan 2030

Signature The undersigned hereby applies to become an independent distributor of Morinda, Inc. As an independent distributor, I agree to the Terms and Conditions and in the Morinda Distributor Manual.

TERMS AND AGREEMENT:
Distributor and Morinda Inc. (Morinda) hereby agree to the following terms and conditions:

1. Legal Age. Distributor is of legal age to enter into this Application and Agreement (the "Agreement") in the state in which Distributor resides.
2. Acceptance. This agreement shall be effective upon

608

Digital Signature of Applicant
ez 11 7c 4b c9 00 c3 ap 54 6e 3d c7 9v c4 6a 30 58 bf 5a 1c 71 48 xa ec be f8 dd fd ce lk 17 3d 17 05 c3 po fb 47 37 d3 9c de kc 3b 64 0b cc 4c r2 2d 7e cb c3 po bb 1e mm 37 2b 20 gh 9c 83 ad
803
Certificate of Applicant
r2 d2 75 71 74 30 iv 96 8f gh 47 ee 43 9v 71 ec 27 81 6d 16 5b ee ek e4 e5 81 9c c2 30 52 1v f9 bc 6v qp 06 02 dc 15 d1 38 80 41 9m mc 5a dc d8 54 97 c3 po 8d 7c ca 2a 2c 7c fl dw r2 d2 fe 54
804

FIG. 8B

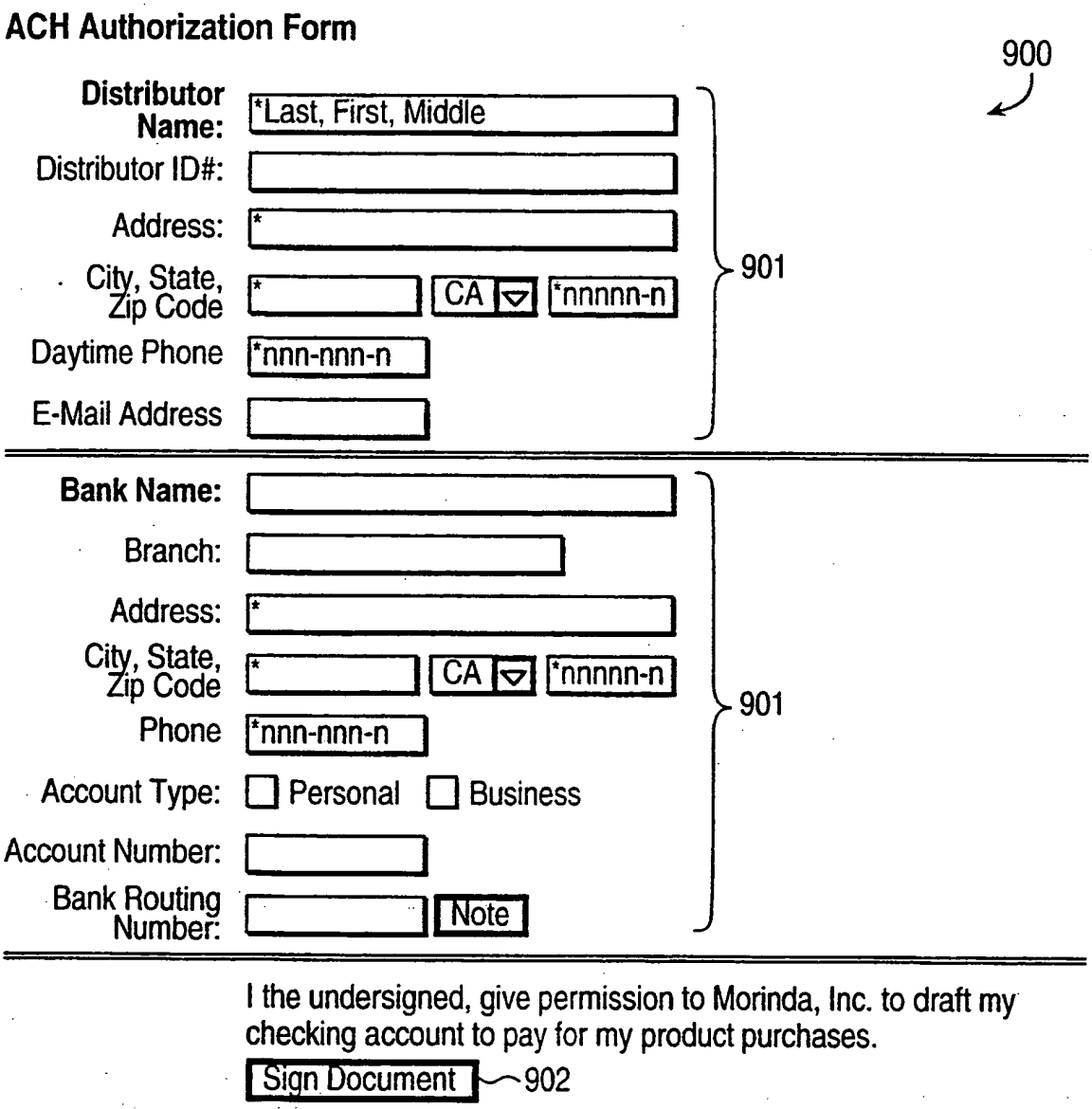

ACH Authorization Form
900
Distributor Name:
*Last, First, Middle
Distributor ID#:
Address:
City, State, Zip Code
CA
*nnnnn-n
Daytime Phone
*nnn-nnn-n
E-Mail Address
901
Bank Name:
Branch:
Address:
City, State, Zip Code
CA
*nnnnn-n
Phone
*nnn-nnn-n
Account Type:
Personal
Business
Account Number:
Bank Routing Number:
Note
901
I the undersigned, give permission to Morinda, Inc. to draft my checking account to pay for my product purchases.
Sign Document
902

FIG. 9

Case AutoShip Change and Enrollment Form

1000

Distributor Name: *Last, First, Middle

Distributor ID#:

Address: *

City, State, Zip Code * CA *nnnnn-n

Daytime Phone *nnn-nnn-n

FAX nnn-nnn-nn

E-Mail Address

1001

Change or Enrollment Request

☐ Enroll me in Morinda's Case AutoShip Program. I understand that I may order any products from Morinda's Case AutoShip Catalog to meet this requirement. I further understand that in order to fully qualify as a Case AutoShip Distributor, my orders for the month must equal or exceed 120 QPV.

Note: Orders from Morinda's Case AutoShip Catalog, *must be made prior to the 15th of each month.* If your orders made prior to that date do not equal 120QPV, you will automatically be sent 1 case (4 bottles) of TAHITIAN NONI® juice.
ACH will be shipped one week after Credit Card orders are shipped.

☐ I prefer Kosher TAHITIAN NONI® juice. I understand that the cost of Kosher TAHITIAN NONI® juice is $124.00 per case.

☐ I would like my case of TAHITIAN NONI® juice regardless of any other purchases. (If checked, fill out payment information below).

1002

I authorize Morinda® to send me ☐ case(s) of TAHITIAN NONI® juice OR ☐ case(s) of Kosher TAHITIAN NONI® juice each month regardless of any other purchases made under my ID Number during any month.

Hawaii, Puerto Rico, Alaska & Guam Only

Please check one of the following:

☐ I will pick up my AutoShip from a local warehouse

☐ I would like my AutoShip to be shipped to my shipping address

1002

FIG. 10A

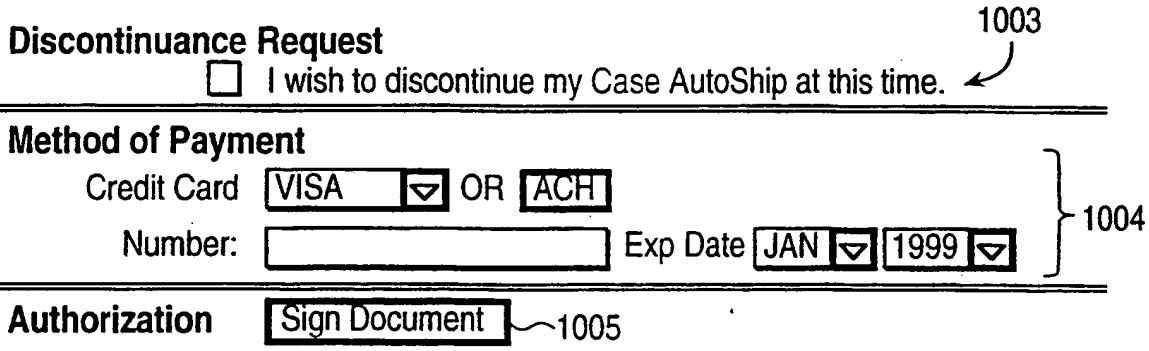

Discontinuance Request
1003
I wish to discontinue my Case AutoShip at this time.
Method of Payment
Credit Card
VISA
OR
ACH
Number:
Exp Date
JAN
1999
1004
Authorization
Sign Document
1005

FIG. 10B

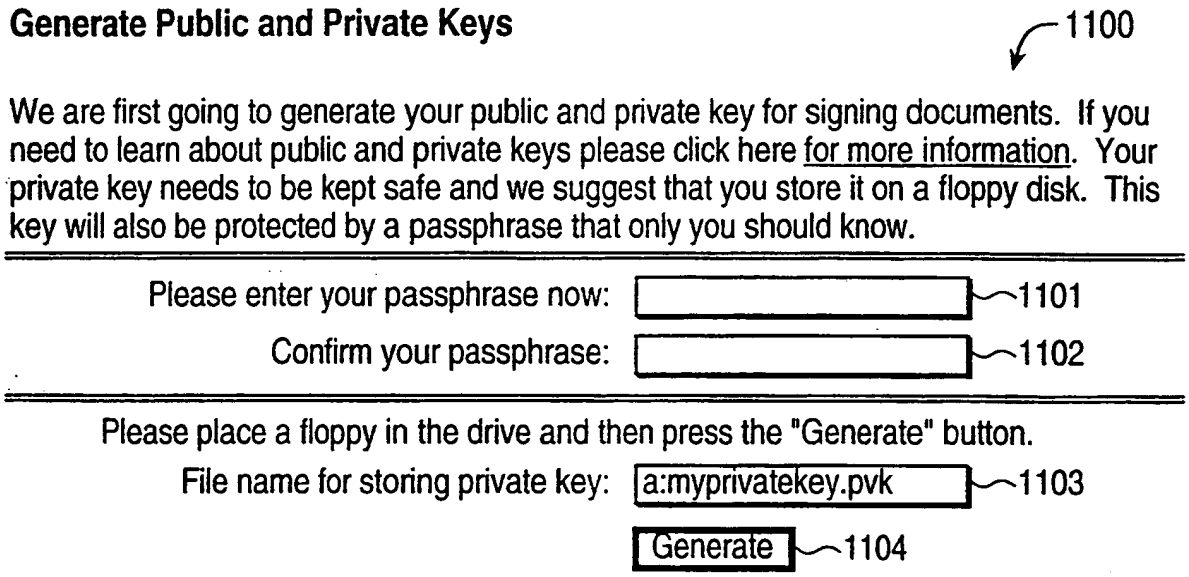

Generate Public and Private Keys
1100
We are first going to generate your public and private key for signing documents. If you need to learn about public and private keys please click here for more information. Your private key needs to be kept safe and we suggest that you store it on a floppy disk. This key will also be protected by a passphrase that only you should know.
Please enter your passphrase now:
1101
Confirm your passphrase:
1102
Please place a floppy in the drive and then press the "Generate" button.
File name for storing private key:
a:myprivatekey.pvk
1103
Generate
1104

FIG. 11

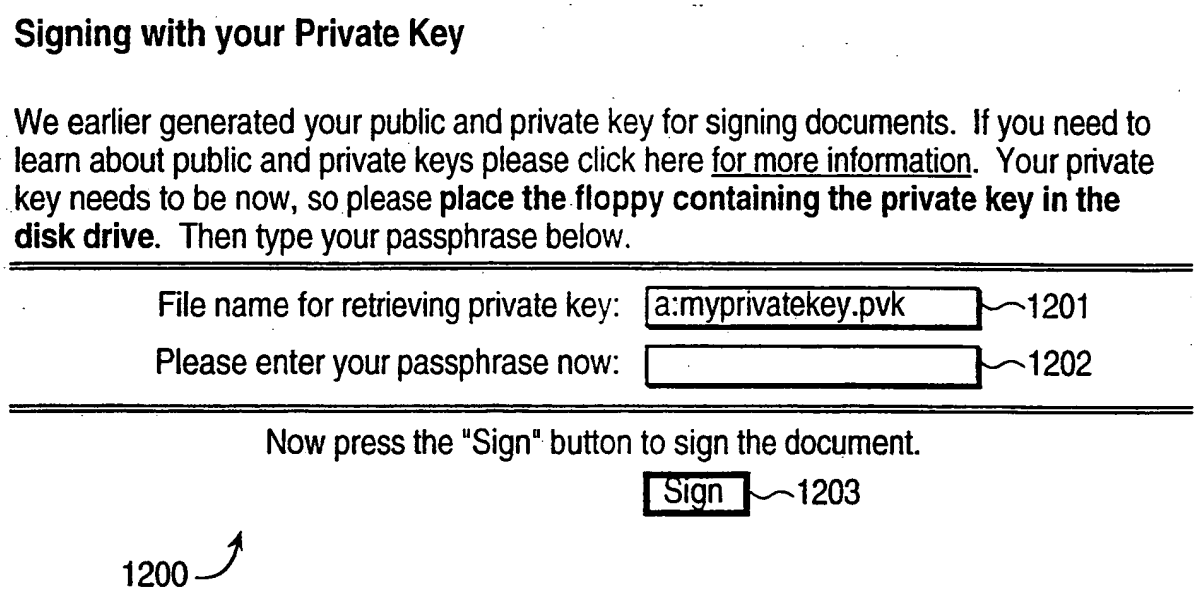

Signing with your Private Key
We earlier generated your public and private key for signing documents. If you need to learn about public and private keys please click here for more information. Your private key needs to be now, so please place the floppy containing the private key in the disk drive. Then type your passphrase below.
File name for retrieving private key:
a:myprivatekey.pvk
1201
Please enter your passphrase now:
1202
Now press the "Sign" button to sign the document.
Sign
1203
1200

FIG. 12

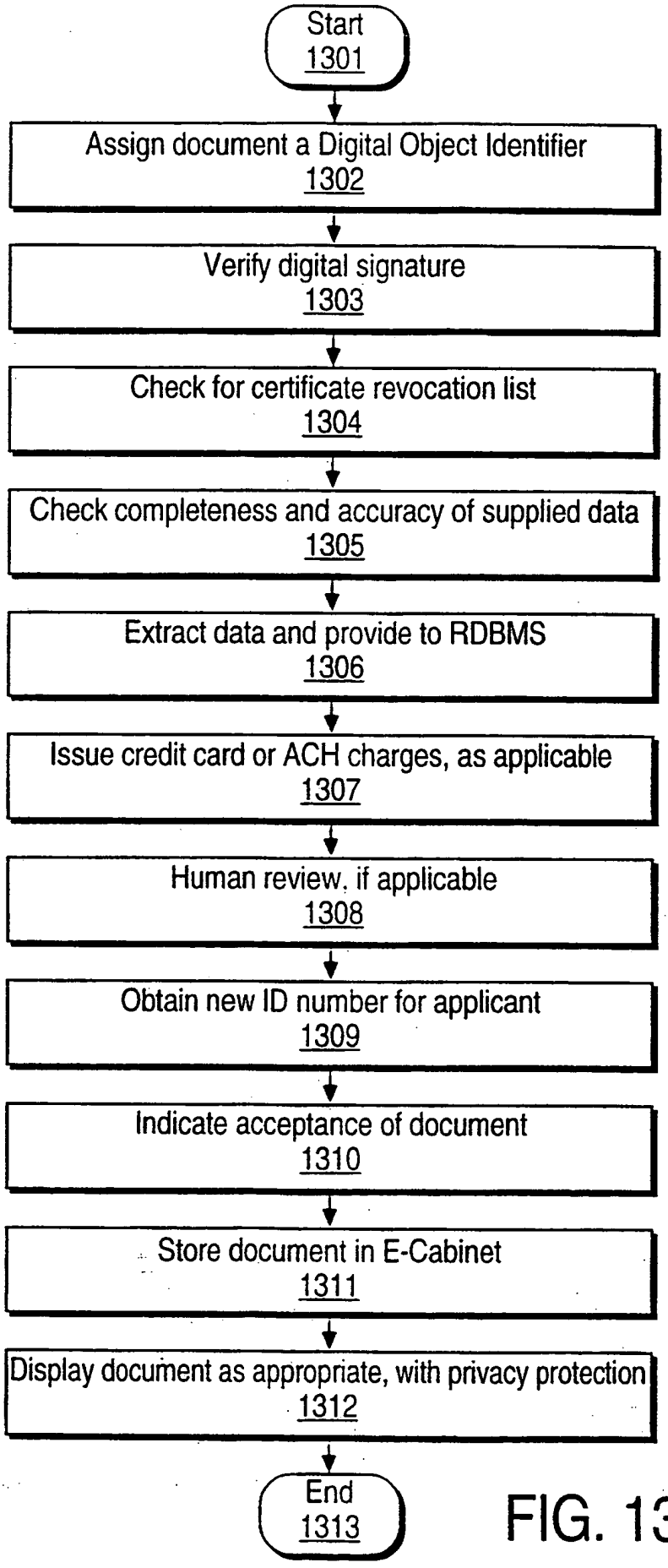

Start
1301
Assign document a Digital Object Identifier
1302
Verify digital signature
1303
Check for certificate revocation list
1304
Check completeness and accuracy of supplied data
1305
Extract data and provide to RDBMS
1306
Issue credit card or ACH charges, as applicable
1307
Human review, if applicable
1308
Obtain new ID number for applicant
1309
Indicate acceptance of document
1310
Store document in E-Cabinet
1311
Display document as appropriate, with privacy protection
1312
End
1313

FIG. 13

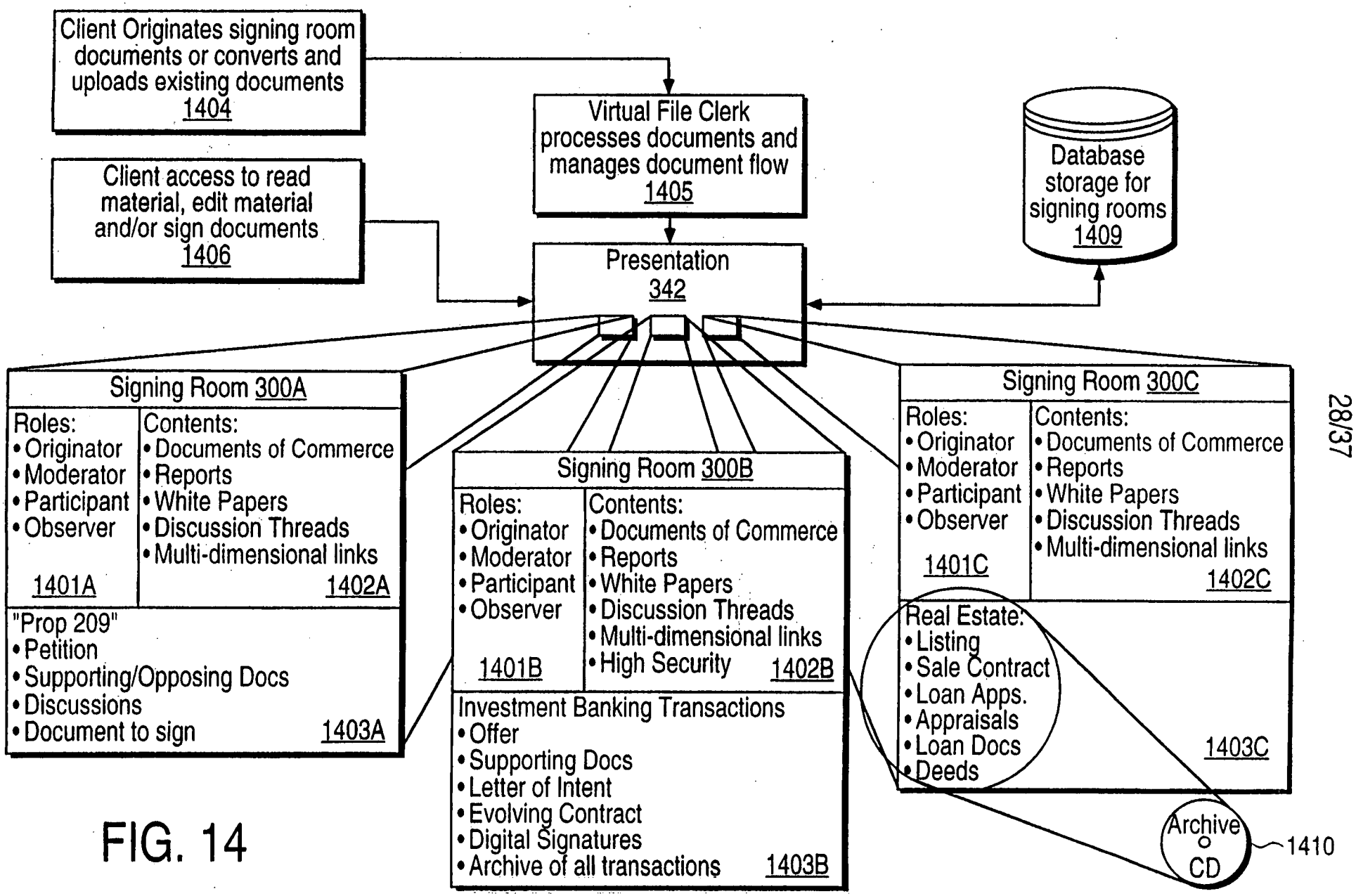

Client Originates signing room documents or converts and uploads existing documents 1404
Client access to read material, edit material and/or sign documents 1406
Virtual File Clerk processes documents and manages document flow 1405
Presentation 342
Database storage for signing rooms 1409
Signing Room 300A
Roles:
• Originator
• Moderator
• Participant
• Observer
1401A
Contents:
• Documents of Commerce
• Reports
• White Papers
• Discussion Threads
• Multi-dimensional links
1402A
"Prop 209"
• Petition
• Supporting/Opposing Docs
• Discussions
• Document to sign
1403A
Signing Room 300B
Roles:
• Originator
• Moderator
• Participant
• Observer
1401B
Contents:
• Documents of Commerce
• Reports
• White Papers
• Discussion Threads
• Multi-dimensional links
• High Security
1402B
Investment Banking Transactions
• Offer
• Supporting Docs
• Letter of Intent
• Evolving Contract
• Digital Signatures
• Archive of all transactions
1403B
Signing Room 300C
Roles:
• Originator
• Moderator
• Participant
• Observer
1401C
Contents:
• Documents of Commerce
• Reports
• White Papers
• Discussion Threads
• Multi-dimensional links
1402C
Real Estate:
• Listing
• Sale Contract
• Loan Apps.
• Appraisals
• Loan Docs
• Deeds
1403C
Archive
CD
1410

FIG. 14

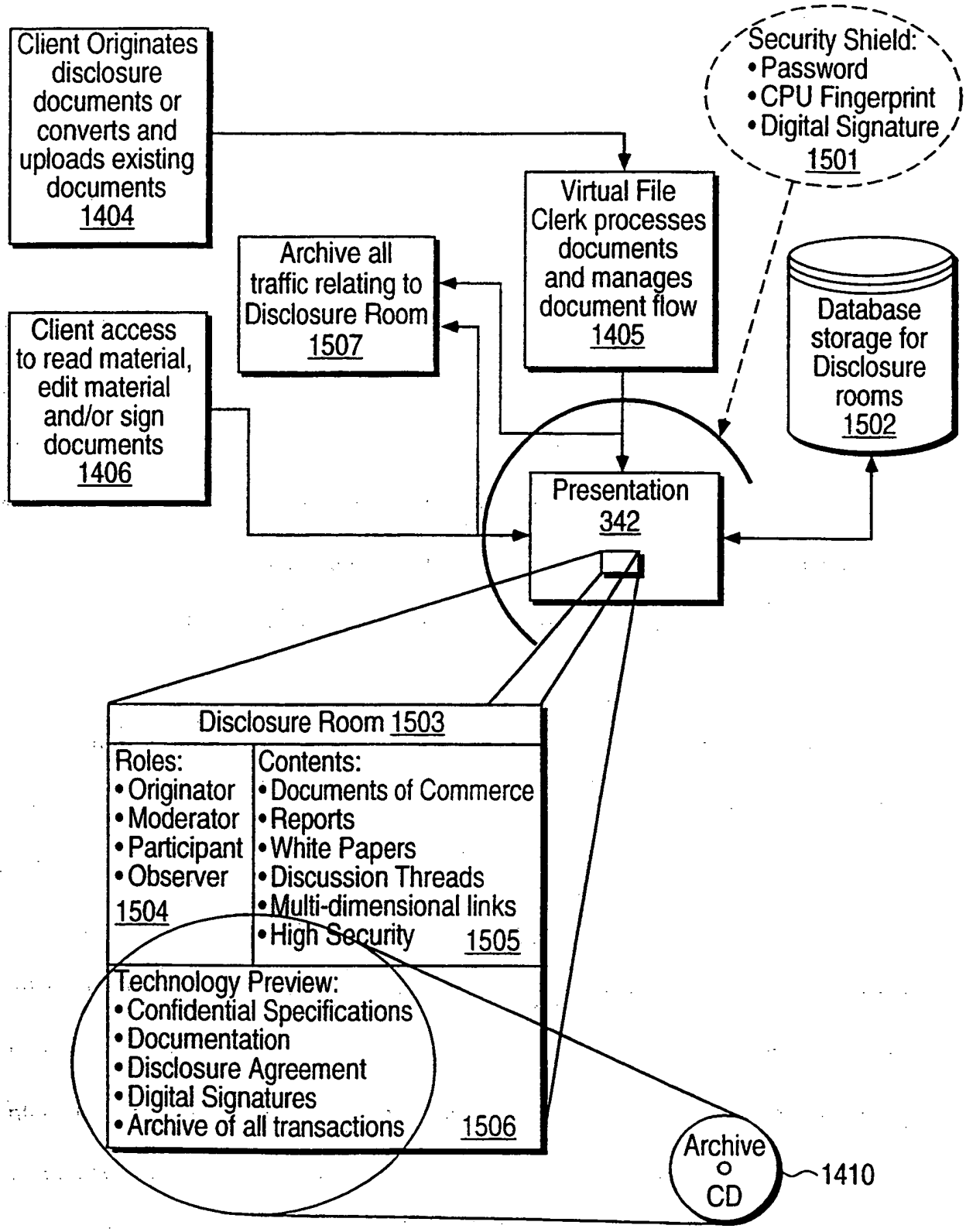

Client Originates disclosure documents or converts and uploads existing documents 1404
Security Shield:
• Password
• CPU Fingerprint
• Digital Signature
1501
Virtual File Clerk processes documents and manages document flow 1405
Archive all traffic relating to Disclosure Room 1507
Database storage for Disclosure rooms 1502
Client access to read material, edit material and/or sign documents 1406
Presentation 342
Disclosure Room 1503
Roles:
• Originator
• Moderator
• Participant
• Observer
1504
Contents:
• Documents of Commerce
• Reports
• White Papers
• Discussion Threads
• Multi-dimensional links
• High Security 1505
Technology Preview:
• Confidential Specifications
• Documentation
• Disclosure Agreement
• Digital Signatures
• Archive of all transactions 1506
Archive CD
1410

FIG. 15

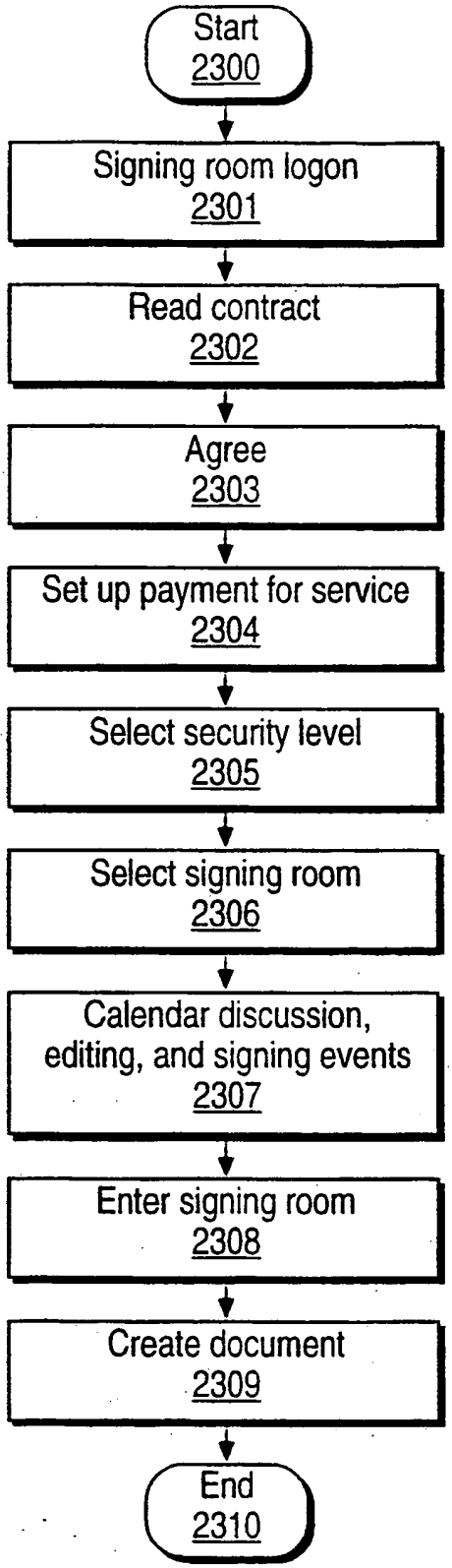

Start
2300
Signing room logon
2301
Read contract
2302
Agree
2303
Set up payment for service
2304
Select security level
2305
Select signing room
2306
Calendar discussion, editing, and signing events
2307
Enter signing room
2308
Create document
2309
End
2310

FIG. 16A

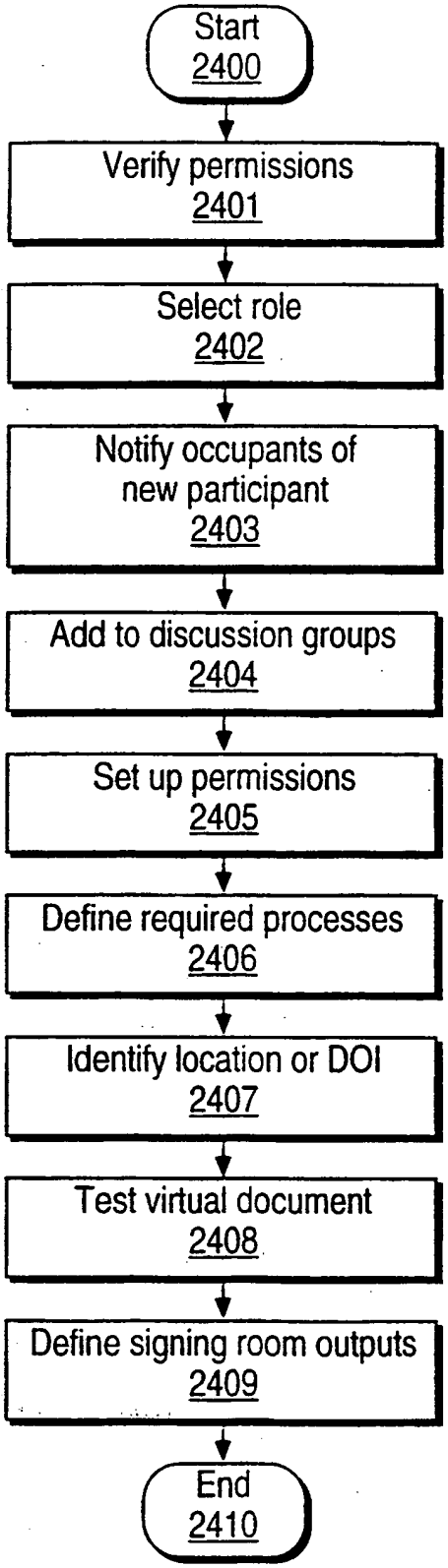

Start
2400
Verify permissions
2401
Select role
2402
Notify occupants of new participant
2403
Add to discussion groups
2404
Set up permissions
2405
Define required processes
2406
Identify location or DOI
2407
Test virtual document
2408
Define signing room outputs
2409
End
2410

FIG. 16B

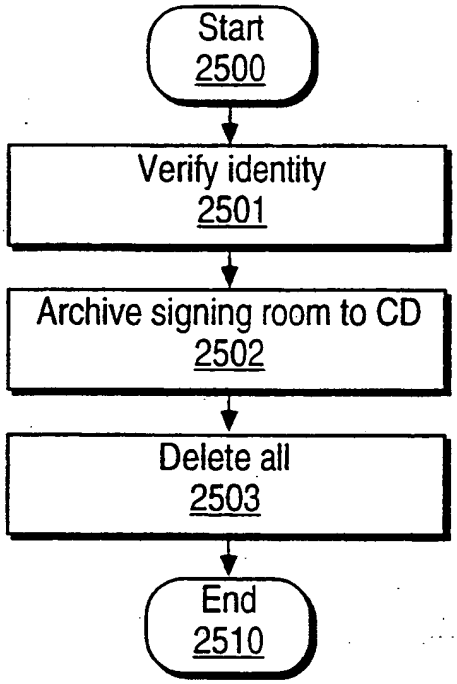

Start
2500
Verify identity
2501
Archive signing room to CD
2502
Delete all
2503
End
2510

FIG. 16C

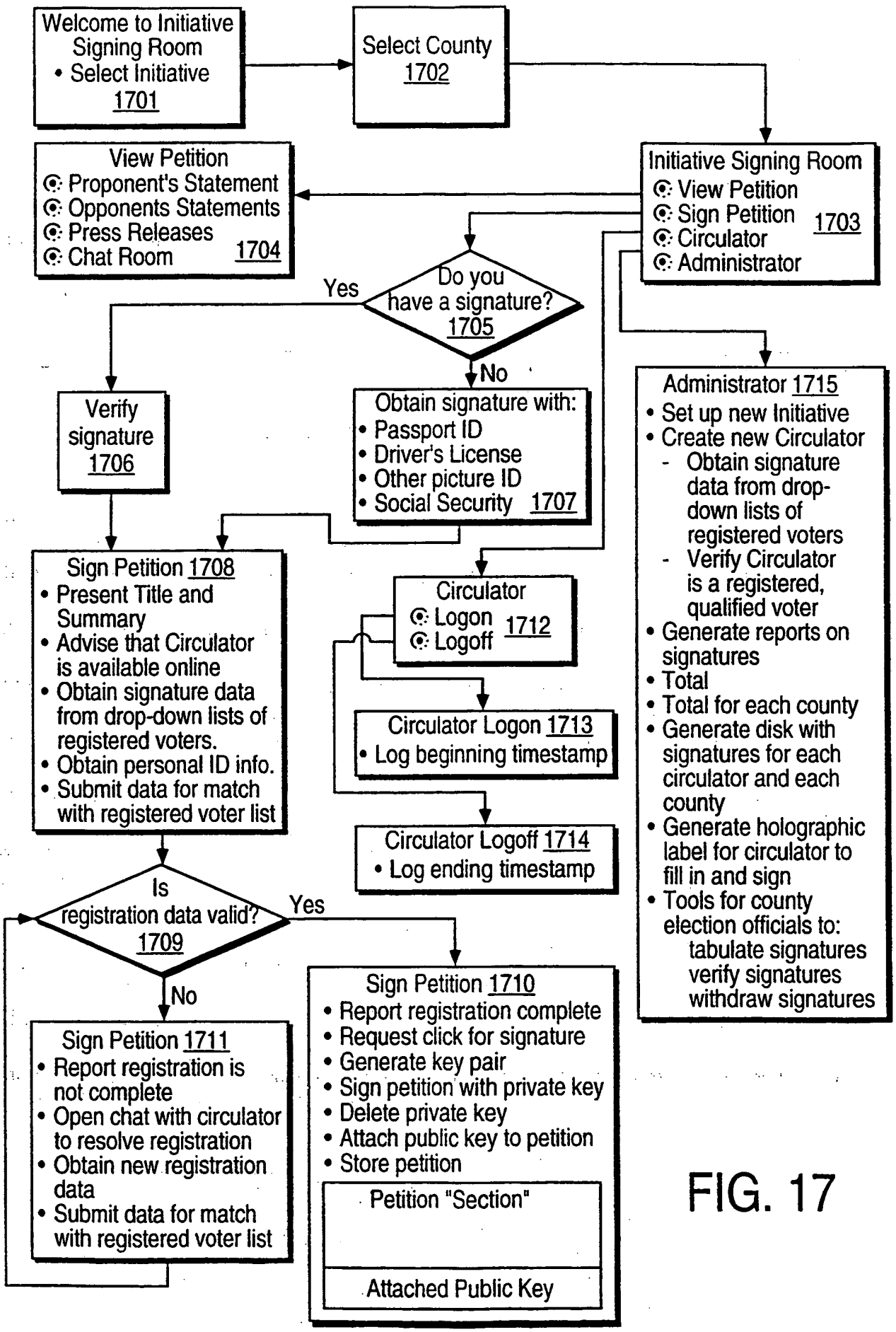

Welcome to Initiative Signing Room
• Select Initiative
1701
Select County
1702
View Petition
Proponent's Statement
Opponents Statements
Press Releases
Chat Room
1704
Initiative Signing Room
View Petition
Sign Petition
Circulator
Administrator
1703
Yes
Do you have a signature?
1705
No
Verify signature
1706
Obtain signature with:
• Passport ID
• Driver's License
• Other picture ID
• Social Security
1707
Administrator 1715
• Set up new Initiative
• Create new Circulator
- Obtain signature data from drop-down lists of registered voters
- Verify Circulator is a registered, qualified voter
• Generate reports on signatures
• Total
• Total for each county
• Generate disk with signatures for each circulator and each county
• Generate holographic label for circulator to fill in and sign
• Tools for county election officials to:
tabulate signatures
verify signatures
withdraw signatures
Sign Petition 1708
• Present Title and Summary
• Advise that Circulator is available online
• Obtain signature data from drop-down lists of registered voters.
• Obtain personal ID info.
• Submit data for match with registered voter list
Circulator
Logon
Logoff
1712
Circulator Logon 1713
• Log beginning timestamp
Circulator Logoff 1714
• Log ending timestamp
Is registration data valid?
1709
Yes
No
Sign Petition 1710
• Report registration complete
• Request click for signature
• Generate key pair
• Sign petition with private key
• Delete private key
• Attach public key to petition
• Store petition
Petition "Section"
Attached Public Key
Sign Petition 1711
• Report registration is not complete
• Open chat with circulator to resolve registration
• Obtain new registration data
• Submit data for match with registered voter list

FIG. 17

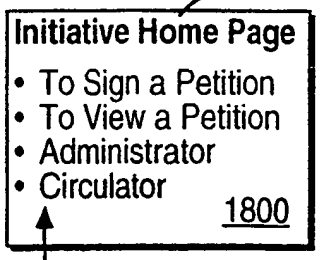


FIG. 18A

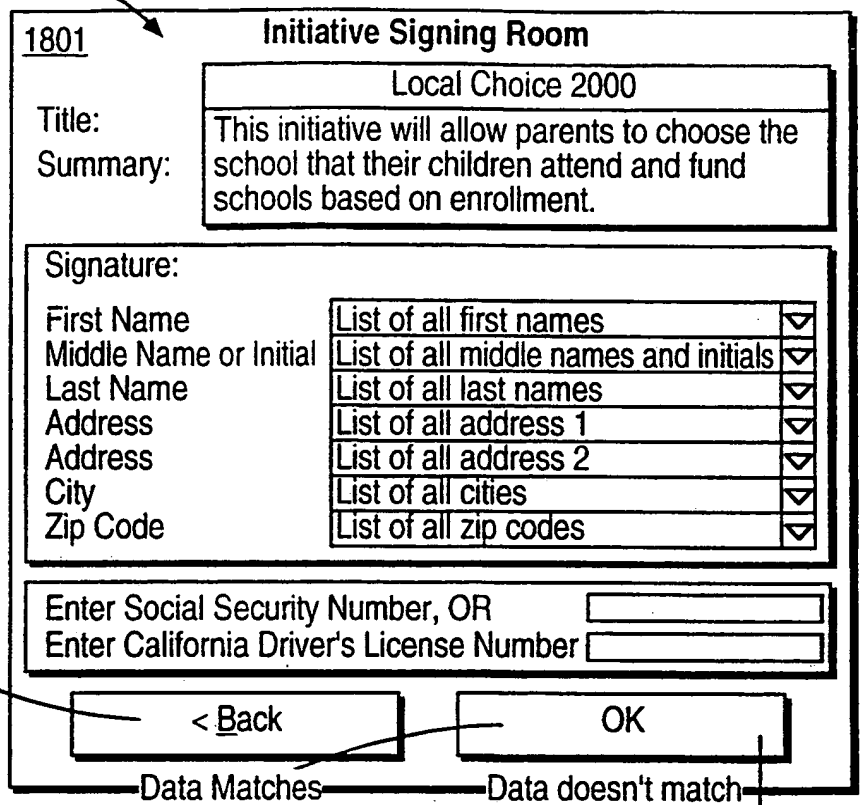


FIG. 18B

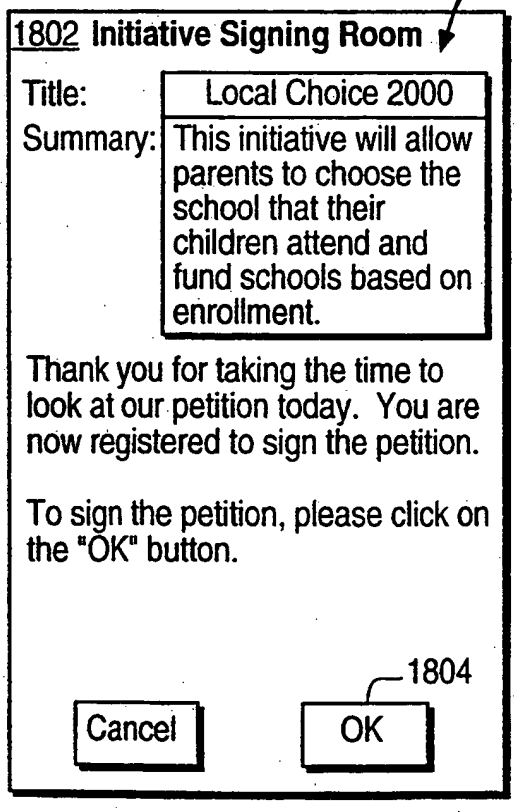


FIG. 18C

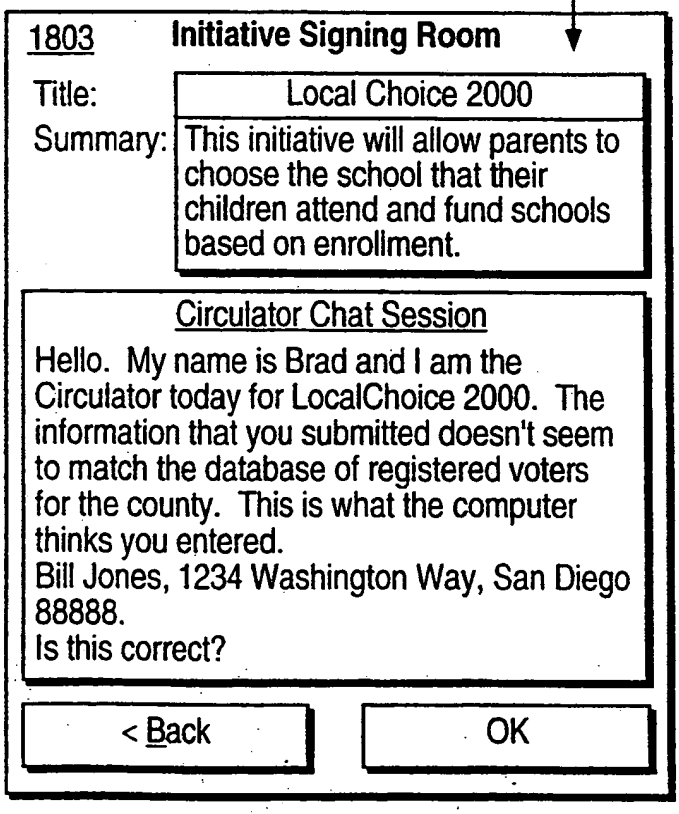


FIG. 18D

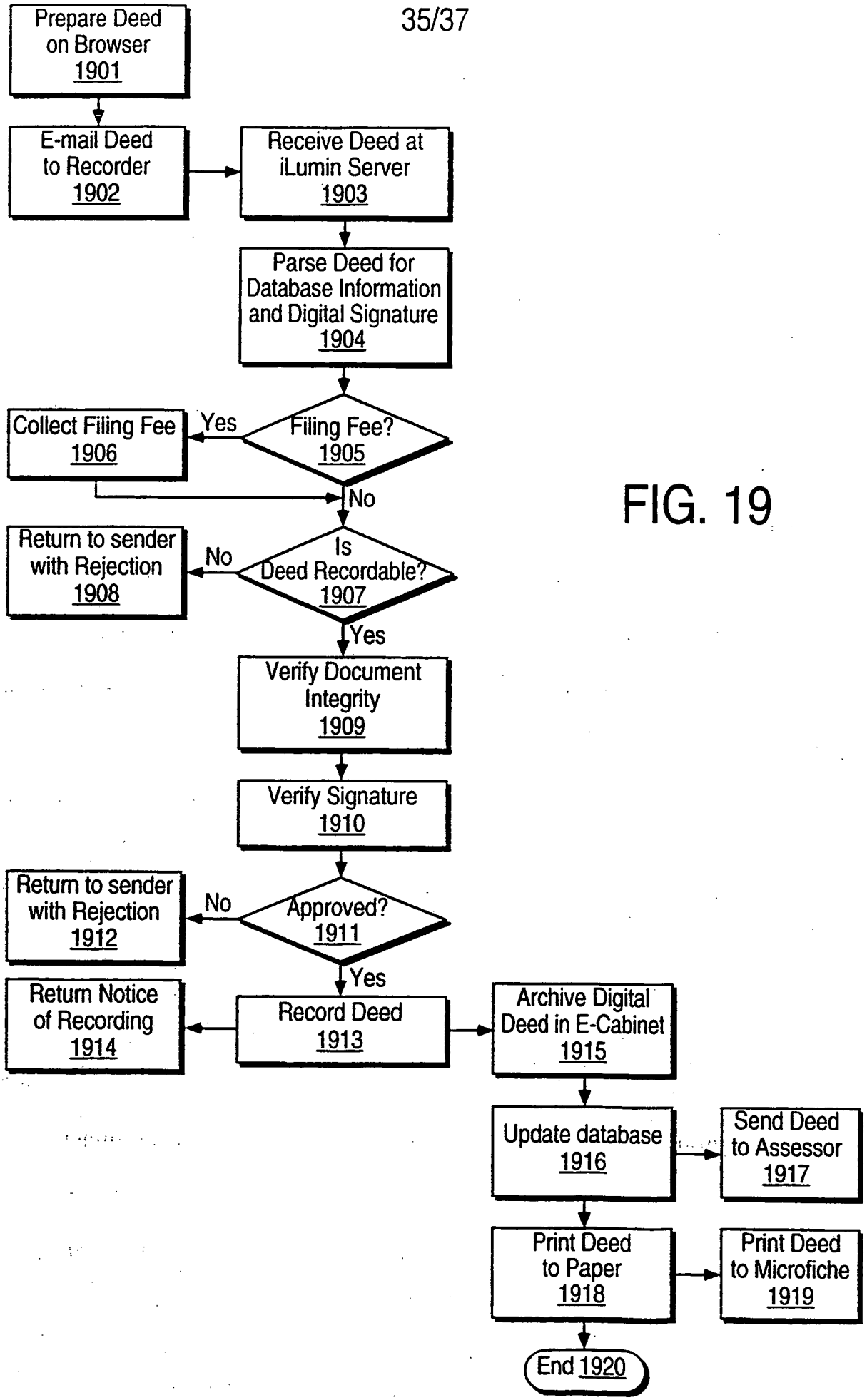

Prepare Deed on Browser 1901
E-mail Deed to Recorder 1902
Receive Deed at iLumin Server 1903
Parse Deed for Database Information and Digital Signature 1904
Filing Fee? 1905
Yes
Collect Filing Fee 1906
No
Is Deed Recordable? 1907
No
Return to sender with Rejection 1908
Yes
Verify Document Integrity 1909
Verify Signature 1910
Approved? 1911
No
Return to sender with Rejection 1912
Yes
Record Deed 1913
Return Notice of Recording 1914
Archive Digital Deed in E-Cabinet 1915
Update database 1916
Send Deed to Assessor 1917
Print Deed to Paper 1918
Print Deed to Microfiche 1919
End 1920

FIG. 19

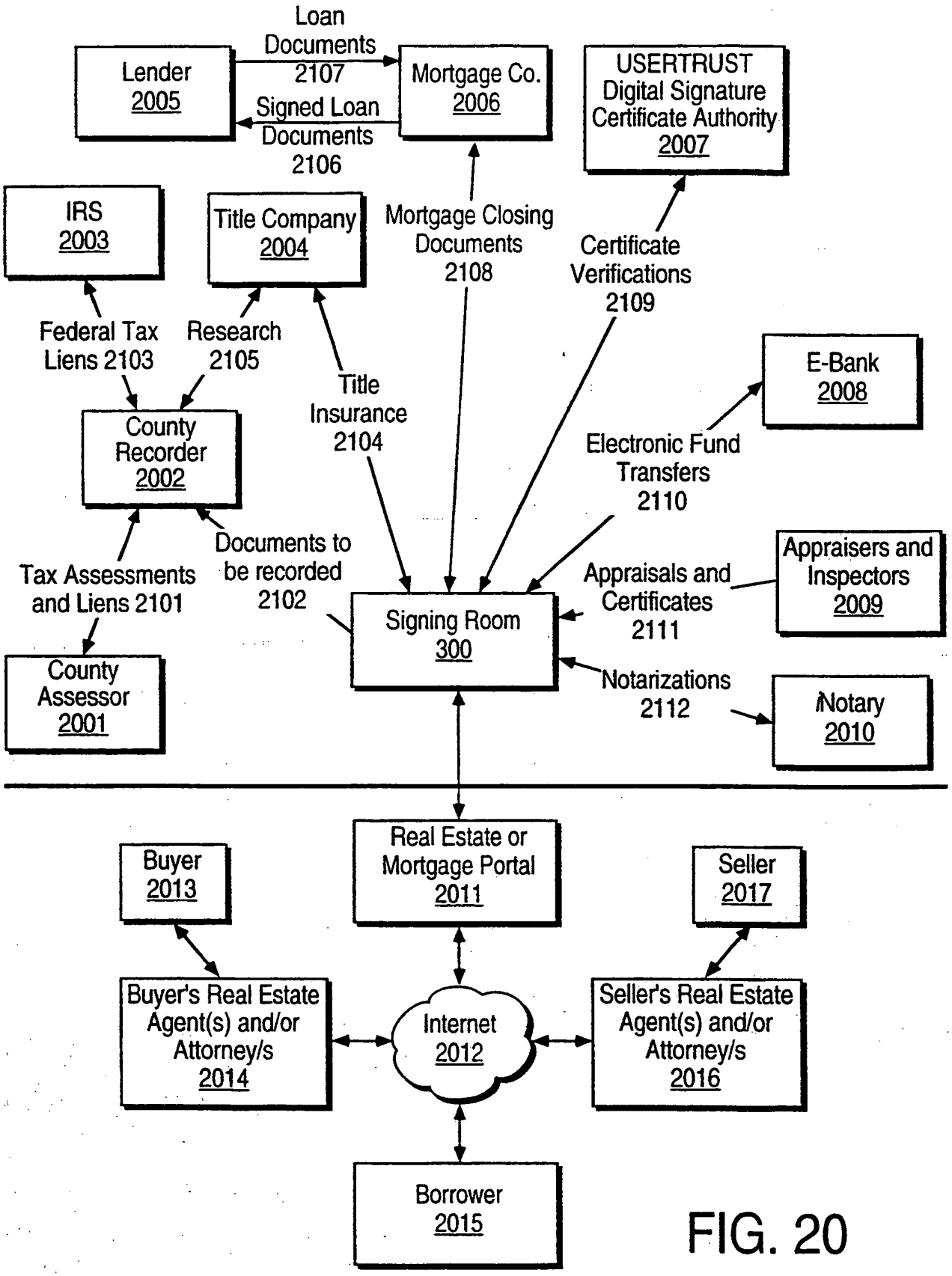

Loan Documents 2107
Signed Loan Documents 2106
Lender 2005
Mortgage Co. 2006
USERTRUST Digital Signature Certificate Authority 2007
IRS 2003
Title Company 2004
Mortgage Closing Documents 2108
Certificate Verifications 2109
Federal Tax Liens 2103
Research 2105
Title Insurance 2104
E-Bank 2008
County Recorder 2002
Electronic Fund Transfers 2110
Tax Assessments and Liens 2101
Documents to be recorded 2102
Appraisers and Inspectors 2009
Appraisals and Certificates 2111
Signing Room 300
County Assessor 2001
Notarizations 2112
Notary 2010
Real Estate or Mortgage Portal 2011
Buyer 2013
Seller 2017
Buyer's Real Estate Agent(s) and/or Attorney/s 2014
Internet 2012
Seller's Real Estate Agent(s) and/or Attorney/s 2016
Borrower 2015

FIG. 20

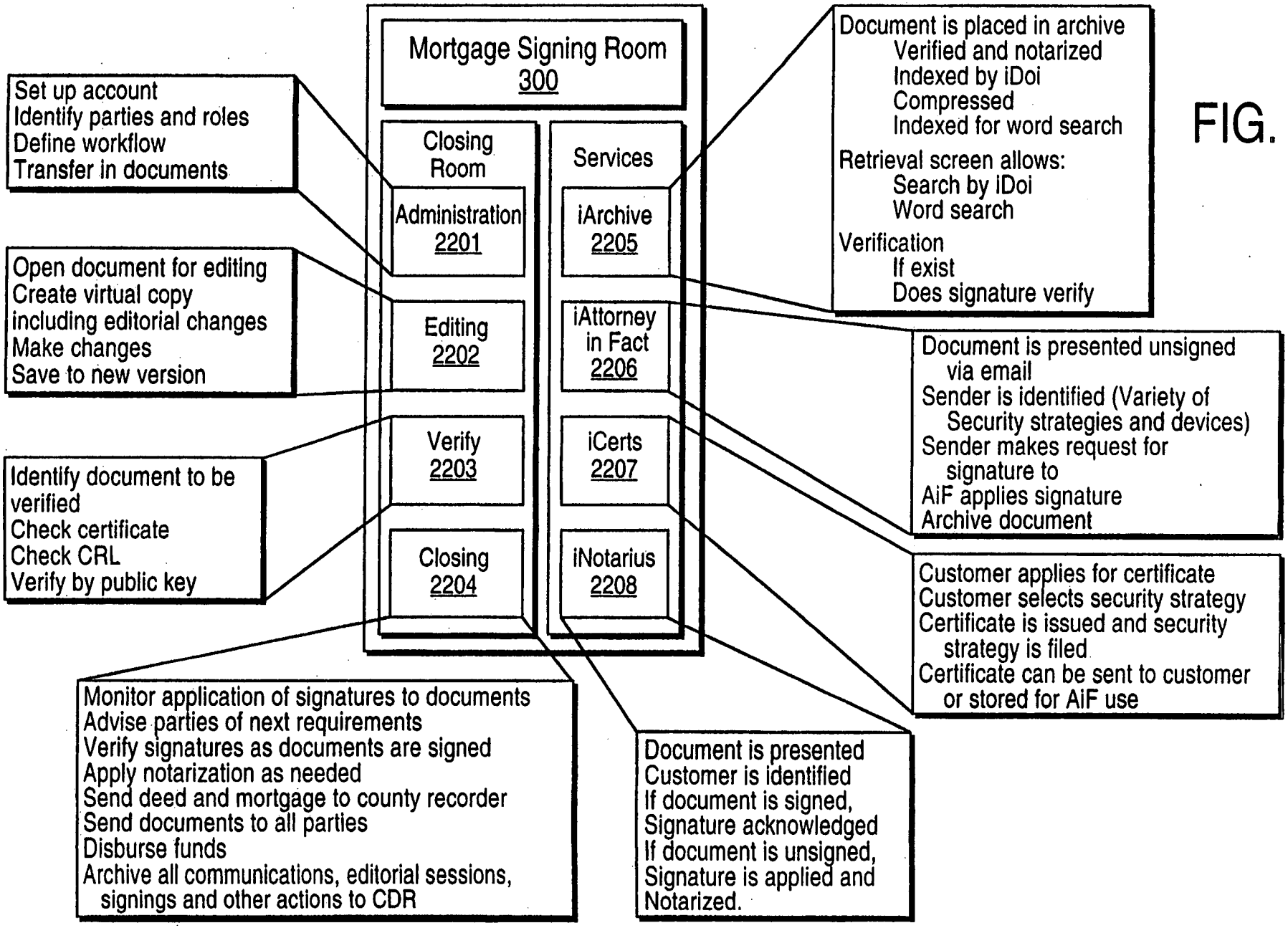


FIG. 21

SUBSTITUTE SHEET (RULE 26)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/10066

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/60 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 34167 A (WEBBER DONALD GARY JR) 6 August 1998 (1998-08-06)	1-3
A	abstract page 14, line 10 -page 20, line 14 page 40, line 27 -page 42, line 4 figures 1,2	4

X	WO 98 01807 A (POLYDOC NV ;RUTTEN HUBERT JOSEPH MARIE (NL); RUYSSEVELT FRANK VAN) 15 January 1998 (1998-01-15)	1,3,4
A	abstract page 1 -page 13, line 26 figure 1A	2

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 July 2000	31/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Jacobs, P

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 387 462 A (IBM) 19 September 1990 (1990-09-19)	1
A	abstract page 3 -page 6 page 12, line 13 page 16 -page 19 page 41 -page 42, line 42	2-4
A	US 5 448 729 A (MURDOCK DAVID M) 5 September 1995 (1995-09-05) abstract column 11, line 31 - line 60 column 15, line 55 -column 17, line 26	1-4
A	BATTLE S A ET AL: "Flexible information presentation with XML" IEE COLLOQUIUM MULTIMEDIA DATABASES AND MPEG-7,GB,IEE, LONDON, 29 January 1999 (1999-01-29), pages 13-1-13-06-6, XP002128574 page 1, paragraph 1 - paragraph 4	2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ional Application No
PCT/US 00/10066

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9834167 A	06-08-1998	AU 6030798 A	25-08-1998
WO 9801807 A	15-01-1998	AU 6245396 A	02-02-1998
		EP 0914637 A	12-05-1999
EP 0387462 A	19-09-1990	DE 68926446 D	13-06-1996
		DE 68926446 T	05-12-1996
		JP 2278458 A	14-11-1990
		US 5315504 A	24-05-1994
US 5448729 A	05-09-1995	US 5317733 A	31-05-1994
		US 5517644 A	14-05-1996

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record.

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.